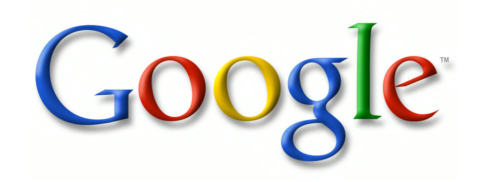
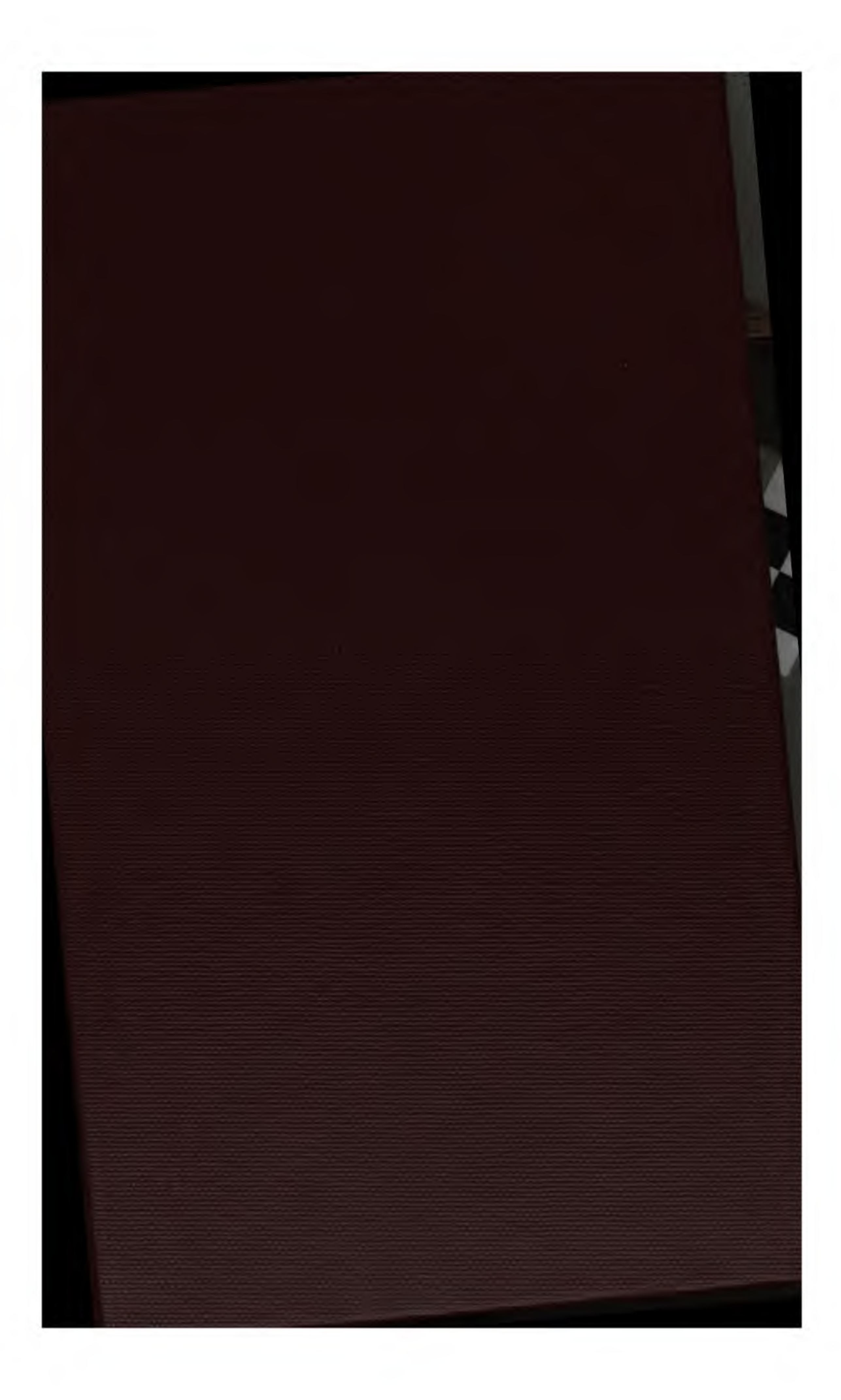








THÉORIE DES NOMBRES.

16597 PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET FILS,
Quai des Grands-Augustins, 55.



THÉORIE DES NOMBRES

PAR

Edouard LUCAS.

> « *Le goût pour les sciences abstraites, en général, et surtout pour les mystères des nombres, est fort rare; on ne s'en étonne pas. Les charmes enchanteurs de cette science sublime ne se décèlent dans toute leur beauté qu'à ceux qui ont le courage de l'approfondir.* »
>
> [Lettre de C.-F. GAUSS à Mlle SOPHIE GERMAIN, du 30 avril 1807].

TOME PREMIER.

LE CALCUL DES NOMBRES ENTIERS. — LE CALCUL DES NOMBRES RATIONNELS.
LA DIVISIBILITÉ ARITHMÉTIQUE.



PARIS,
GAUTHIER-VILLARS ET FILS, IMPRIMEURS-LIBRAIRES
DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.

1891

PRÉFACE.

> « C'est icy un livre de bonne foy, lecteur
> ... Mes deffauts s'y liront au vif.... »
>
> MONTAIGNE, Préface des *Essais*.

Le premier traité d'Arithmétique supérieure, ou d'Arithmologie, a été publié à la fin du siècle dernier par LEGENDRE, sous le titre : *Essai sur la théorie des nombres* (Paris, an VI). Cet excellent ouvrage renfermait non seulement tout ce qui était connu jusqu'alors sur cette science, et notamment les recherches d'EULER et de LAGRANGE, sur les théorèmes énoncés par FERMAT, mais encore les nombreuses découvertes de l'illustre auteur, qui rendit de si grands services à l'Arithmétique. On lui doit surtout le théorème fondamental qui porte son nom, c'est-à-dire la *Loi de réciprocité des résidus quadratiques*. Deux autres éditions, considérablement augmentées, ont été publiées de son vivant; la troisième, définitive, en trois volumes in-4°, en 1830. Celle-ci vient d'être traduite en langue allemande par M. MASER (Leipzick, 1886).

Dans la première année du siècle, GAUSS fit paraître les *Disquisitiones arithmeticæ* (Leipzick, 1801). Une traduction française, les *Recherches arithmétiques* (Paris, 1807), est due à POULLET-DELISLE. Depuis, de nombreuses éditions de cet ouvrage admirable ont été publiées dans plusieurs

langues, et notamment la version originale, en langue allemande, pour laquelle l'auteur n'avait pu trouver d'éditeur!

Ce livre, monument impérissable, dévoile l'immense étendue, l'étonnante profondeur de la pensée humaine. Son auteur excella dans toutes les parties des Sciences mathématiques, pures et appliquées; dans l'Analyse algébrique, dans la Théorie des fonctions, dans le Calcul des probabilités, dans la Géométrie des surfaces, dans l'Astronomie physique et pratique, dans la Mécanique céleste, dans l'Optique, dans le Magnétisme, dans la Théorie des attractions, etc.; ses compatriotes l'ont, avec raison, surnommé *Princeps mathematicorum*. Mais ce que ce savant illustre, que l'on doit placer à côté des plus grands génies scientifiques de l'humanité, préférait par-dessus tout, c'était sa *chère Arithmétique*, ainsi qu'il le répétait continuellement dans sa correspondance; nous n'y contredirons point.

Les découvertes de GAUSS ont donné lieu à de nombreux mémoires sur l'Arithmétique, surtout en Allemagne; mais nous ne pouvons citer ici que les principaux traités didactiques. — En France, POINSOT publie, dans le *Journal de Liouville* (t. X, 1845), un mémoire intitulé : *Réflexions sur les principes fondamentaux de la Théorie des nombres*; cet ouvrage mérite l'attention à plus d'un titre, surtout par la clarté et l'élégance de l'exposition, mais non par la nouveauté; malheureusement, la démonstration du principe, sur lequel repose tout l'ensemble, n'est pas rigoureuse, bien que toutes les conséquences en soient exactes. — Nous devons rappeler encore les deux opuscules de LEBESGUE : *Exercices d'Analyse numérique* et *Introduction à la Théorie des nombres* (Paris, 1859 et 1868). On doit regretter que cet

auteur n'ait pu terminer la publication qu'il avait annoncée. — Enfin le second volume du *Cours d'Algèbre supérieure,* de SERRET (4e édition), est consacré presque entièrement à la théorie des congruences et à ses applications à la résolution algébrique des équations; mais, par suite d'une inadvertance inconcevable, dès la première page, plusieurs des démonstrations présentées par l'auteur manquent de rigueur. En particulier, nous signalerons comme imparfaite la démonstration du théorème de BACHET, que tout entier est la somme de quatre carrés, ou de moins de quatre. Cette critique n'a pas pour but de diminuer l'importance de l'excellent ouvrage de SERRET, qui d'ailleurs a été apprécié, traduit et publié en Allemagne (Leipzick, 1879) par M. WERTHEIM. Nous exposerons, dans le second volume, une fort belle démonstration du théorème de BACHET, qui nous a été communiquée par M. MATROT, ingénieur en chef des Mines.

M. TCHEBYCHEF a publié en langue russe la *Théorie des congruences* (Saint-Pétersbourg, 1847). Une traduction en langue allemande vient de paraître par les soins de M. SCHAPIRA, professeur à l'Université de Heidelberg (Berlin, 1889). Cet ouvrage contient, dans l'original mais non dans la traduction, la démonstration de l'un des plus beaux et des plus difficiles théorèmes de l'Arithmétique transcendante; nous donnerons, dans le troisième volume, une simplification de cette admirable démonstration, qui suffirait à elle seule pour obtenir l'immortalité, si son auteur ne s'était surpassé lui-même par l'invention d'un nouveau genre de calcul, pour la détermination des maxima et des minima d'intégrales comprises entre des limites données, et par ses nombreuses et utiles applications à la Mécanique des systèmes articulés.

Il serait trop long de donner la liste des ouvrages qui ont paru en Allemagne, dans ces dernières années, sur le sujet qui nous occupe. Nous nous bornerons à citer les Leçons de Lejeune-Dirichlet, publiées par M. Dedekind : *Vorlesungen über Zahlentheorie*. La troisième édition de ce délicieux traité (Brunswick, 1881) contient, en dehors de la démonstration du célèbre théorème de Dirichlet sur la présence des nombres premiers dans les progressions arithmétiques, de remarquables et importantes additions de l'éditeur sur l'Arithmétique générale. Pour terminer, nous citerons les Leçons académiques de M. Bachmann sur la dernière section des *Disquisitiones* de Gauss, sous le titre : *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie* (Leipzick, 1872).

Telles sont les principales sources d'où notre œuvre découle.

Depuis longtemps, nous avons amassé et recueilli des documents nombreux, intéressants, de tous auteurs et de tous pays, pour écrire un livre sur le sujet qui nous occupe. Nous y ajoutons une partie de nos propres recherches, que nous avions publiées dans ce but, au jour le jour, un peu partout et notamment dans les *Comptes rendus*, les Bulletins des Académies des Sciences de Turin, Rome et Saint-Pétersbourg, de la Société mathématique de France ; dans l'*American Journal*, à Baltimore, dans les Comptes rendus de l'Association française pour l'Avancement des Sciences, dans les *Nouvelles Annales de Mathématiques*, dans la *Nouvelle Correspondance* et dans *Mathesis*, à Bruxelles et à Liège, dans le *Messenger of Mathematics*, à Cambridge, etc.

Il nous reste à indiquer le plan général de ce livre. Nous

prenons la science à son origine et, dans l'Introduction, nous indiquons les débuts, les progrès et les applications de l'Arithmétique, tout en restant dans les idées générales. Nous compléterons cet exposé, s'il y a lieu, pour les volumes qui suivront. Nous insistons sur les procédés du calcul, d'autant plus qu'on les néglige dans les éléments, à ce point que la construction des tables de multiplication est enseignée d'une manière défectueuse. Nous mettons les calculs dits *algébriques* en face des calculs de l'Arithmétique ordinaire, car nous considérons le nombre entier d'une manière générale, indépendante de son enveloppe, positif ou négatif, soit qu'on le représente par des boules, par des chiffres ou par les lettres de l'alphabet. Ce n'est pas dans la manière de figurer les nombres, de les habiller pour ainsi dire, que nous distinguons l'Arithmétique de l'Algèbre, mais c'est surtout dans l'essence même des nombres, dans la manière de les concevoir. La ligne de démarcation entre l'Arithmétique et l'Algèbre provient de l'idée que l'on se fait du nombre, suivant qu'on le considère comme grandeur, ou simplement comme numéro d'ordre, c'est-à-dire suivant que l'on accepte ou que l'on refuse la notion de continuité ; c'est ainsi que la doctrine des nombres irrationnels, des logarithmes, etc., appartient exclusivement au domaine de l'Algèbre, c'est-à-dire des fonctions analytiques.

Pour tout ce qui concerne les éléments du calcul, numérique ou littéral, les développements marchent parallèlement, quand on exclut la continuité. A toutes les opérations du calcul décimal correspondent les opérations analogues du calcul sur les polynômes et ainsi pour la multiplication et pour la division, pour la recherche des diviseurs et des mul-

tiples communs des nombres et des polynômes entiers, pour la décomposition en fractions simples et pour le développement en fractions continues des nombres fractionnaires et des fractions rationnelles, pour la décomposition d'un nombre entier en facteurs premiers et d'un polynôme en facteurs irréductibles, etc. Mais il existe une différence profonde entre ces deux calculs, aussitôt que l'on introduit la notion de continuité et, par suite, d'incommensurabilité; nous citerons quelques exemples.

Dans la théorie des équations algébriques, les théorèmes de DESCARTES et de NEWTON (¹), de ROLLE et de STURM apprennent à connaître le nombre des racines réelles d'une équation, comprises entre deux limites données; mais il n'existe, quant à présent, rien de pareil en Arithmétique, et nous ne connaissons aucun procédé de calcul pour déterminer le nombre des facteurs premiers d'un entier donné compris entre deux limites. La méthode de HUDDE, dite *des racines égales*, permet de décomposer tout polynôme contenant des facteurs multiples; mais il n'existe aucun procédé pour connaître les facteurs multiples d'un entier donné. Enfin la théorie des fonctions donne naissance, par les développements en séries, à des suites de nombres, qui sont les coefficients des puissances des variables; mais la formation de ces coefficients et leurs propriétés appartiennent essentiellement à l'Arithmétique, lorsque l'on peut former ces nombres, indépendam-

(¹) Le théorème de DESCARTES donne une limite supérieure des racines réelles d'une équation par le compte des variations, c'est-à-dire des successions des signes de tous les ensembles formés par *deux* termes consécutifs; dans le théorème de NEWTON, on considère les ensembles de *trois* termes consécutifs. La démonstration de ce dernier théorème a été donnée pour la première fois par M. SYLVESTER.

ment de toute considération de continuité, par des opérations rationnelles. C'est ainsi que nous avons pu exposer le calcul et les propriétés de ces coefficients, mystérieux comme les nombres premiers, que l'on appelle *nombres* de BERNOULLI, d'EULER, de GENOCCHI, d'HAMILTON, etc.

Comme toutes les sciences, l'Arithmétique résulte de l'observation; elle progresse par l'étude des phénomènes numériques donnés par des calculs antérieurs, ou fabriqués, pour ainsi dire, par l'expérimentation; mais elle n'exige aucun laboratoire et possède seule le privilège de convertir ses inductions en théorèmes déductifs. Comme en Chimie, par exemple, on prépare les nombres au moyen du calcul; par la divisibilité, on décompose ceux-ci en éléments simples, les facteurs premiers; par la théorie des résidus potentiels, on détermine leur aspect et, en quelque sorte, leurs réactions mutuelles; enfin, par la juxtaposition des nombres triangulaires, carrés, polygonaux, cubiques, etc., la théorie des formes numériques rappelle l'étude des systèmes cristallins. C'est par l'observation du dernier chiffre dans les puissances successives des nombres entiers que FERMAT, notre *Divus Arithmeticus,* créa l'Arithmétique supérieure, en donnant l'énoncé d'un théorème fondamental; c'est par la méthode expérimentale, en recherchant la démonstration de cette proposition, que la théorie des racines primitives fut imaginée par EULER; c'est par l'emploi immédiat de ces racines primitives que GAUSS obtint son célèbre théorème sur la division de la circonférence en parties égales, et celui-ci fut le point de départ des profondes recherches d'ABEL et de GALOIS, de MM. KUMMER, HERMITE et KRONECKER, dans l'Algèbre supérieure.

Nous n'avons pas la prétention de comparer nos modestes découvertes à celles de tous ces savants immortels; mais c'est encore par l'observation de la suite de FIBONACCI

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ \ldots,$$

dans laquelle chaque terme est la somme des deux termes qui le précèdent, que nous avons rencontré une proposition nouvelle qui constitue la réciproque du théorème de FERMAT. Nous en avons déduit un grand nombre de corollaires qui permettent de savoir si un nombre donné p de vingt ou trente chiffres est premier ou non, lorsque l'on connaît la décomposition en facteurs premiers de l'un des nombres $(p \pm 1)$ qui le comprennent. Par l'emploi de ce nouveau procédé, nous avons énoncé un grand nombre de théorèmes analogues à celui de WILSON et obtenu des nombres premiers de vingt et de trente chiffres, tandis que le plus grand nombre premier connu, il y a vingt ans, $(2^{31} - 1)$ indiqué par EULER, n'en avait que dix. Ainsi, par exemple, on a la proposition suivante qui vient compléter le théorème de GAUSS dans la théorie de la division de la circonférence : *Pour que le nombre*

$$2^{2^n} + 1$$

soit premier, il faut et il suffit qu'il divise le nombre

$$3^{2^{2^n}} + 1.$$

La théorie des suites récurrentes est une mine inépuisable qui renferme toutes les propriétés des nombres; en calculant les termes successifs de telles suites, en décomposant ceux-ci en facteurs, en recherchant par l'expérimentation les lois de l'*apparition* et de la *reproduction* des nombres premiers, on fera progresser d'une manière systématique l'étude des pro-

priétés des nombres et de leurs applications dans toutes les branches des Mathématiques.

Nous avons donc exposé l'ensemble des vérités fondamentales du Calcul et de l'Arithmétique, d'après le mode analytique, en laissant de côté toute préoccupation de programmes officiels. Puisque toutes nos opérations et tous nos raisonnements ne portent que sur les nombres entiers, indépendamment de toute considération de continuité ou d'irrationnalité, nous faisons abstraction des nombres qui entrent dans les formules, pour ne voir que l'ordre de succession des opérations que l'on applique à ces nombres, d'une manière effective ou supposée. Nous rangeons ces opérations dans un ordre naturel, logique, tel que chacun des signes et des symboles d'opération nécessite la connaissance de tous ceux qui le précèdent.

Le signe $+$ de l'addition et son symbole extensif, Σ.

Le signe $-$ de la soustraction et celui des différences successives, Δ.

Le signe $\times$ de la multiplication et de son symbole extensif, Π.

L'exposant des puissances, a^n et le symbole des factorielles, $a^{n/r}$.

Le signe : de la division exacte et les symboles des opérations dans lesquelles on recherche le quotient approché, par excès ou par défaut, et le reste d'une division.

Le symbole de l'opération du plus grand commun diviseur et du développement d'un nombre rationnel en fraction continue.

Le symbole de la recherche des diviseurs d'un nombre. — Le symbole de la recherche des nombres inférieurs et premiers à un nombre donné.

Les symboles de Legendre et de Jacobi dans la théorie des résidus quadratiques, etc., etc.

Après avoir ainsi classé ces opérations, nous les représentons par les lettres de l'alphabet, dans l'ordre ordinaire.

Cela posé, considérons une formule ou un raisonnement quelconque; écrivons dans l'ordre où ils se présentent les différents symboles des opérations fictives ou effectuées, nous formons ainsi un *mot* contenant une ou plusieurs des lettres symboliques, et d'ailleurs ces lettres peuvent entrer plusieurs fois dans le même mot. A chaque formule correspond un mot symbolique et inversement. En rangeant tous ces mots dans l'ordre du dictionnaire, on obtient la succession logique des vérités de l'Arithmétique. Il est évident d'ailleurs qu'une même vérité peut occuper diverses places, suivant le mode de raisonnement que l'on emploie pour sa démonstration; d'autre part, deux questions qui paraissent voisines d'après la nature de leur énoncé peuvent se trouver très éloignées dans le développement de notre ouvrage, lorsque les résultats conduisent à des formules de nature différente. Ainsi, par exemple, lorsque l'on veut déterminer le nombre des dispositions différentes d'objets placés sur un circuit fermé, on doit considérer deux cas suivant que les objets sont tous distincts ou que plusieurs d'entre eux ne le sont pas. Dans le premier cas, on a une formule très simple (n° 42); il n'en est pas de même dans le second et la formule correspondante ne peut trouver sa place que dans le IIIe Livre au Chapitre XXII (voir l'*Addition VII*, p. 501). Il peut encore se présenter d'autres circonstances et, par exemple, dans la théorie des *factorielles*, c'est-à-dire des produits de nombres en progression arithmétique, et dans celle des *puissances*, c'est-à-dire des produits de nombres égaux; ceux-ci reviennent à des factorielles dans lesquelles s'annule la raison r de la progression arithmétique. Souvent, le cas général donne des formules plus simples, tandis que le cas particulier produit des for-

mules illusoires. C'est pour ce motif que nous avons placé parfois le symbole de la factorielle avant celui de la puissance.

En beaucoup d'endroits, nous avons employé dans nos raisonnements le mode de calcul sur l'échiquier, à l'imitation de Pascal, dans son fameux Traité sur le triangle arithmétique. Pour montrer la supériorité de ce procédé général d'Arithmétique de position, nous avons donné, dans le Chapitre sur le *Calcul des probabilités,* les solutions si ingénieuses de M. Delannoy, au sujet du *Scrutin de ballottage* et de la *Durée du Jeu.* Cette méthode donne, quant à présent, l'unique solution d'une question difficile posée par Laplace, tandis que les résultats présentés récemment à l'*Académie des Sciences* ont une forme illusoire.

Dans un but de simplification, nous nous servons de quelques mots nouveaux : d'abord, ceux de *codiviseurs* et de *comultiples,* qui se comprennent d'eux-mêmes ; nous désignons par *indicateur* d'un entier n le nombre des entiers inférieurs à n et premiers avec lui ; nous désignons par le mot *gaussien* de a pour un module donné le plus petit exposant g de a pour lequel $(a^g - 1)$ est un multiple du module ; enfin, avec M. Sylvester, nous appelons *cumulant* le résultat de l'opération du symbole généralisé d'Euler, dans la théorie des fractions continues. — Nous avons employé, pour les raisonnements et les formules, les signes connus, en choisissant toujours ceux qui donnent aux formules la physionomie la plus simple et la plus claire ; nous avons adopté le signe $\equiv$ de la congruence, qui est indispensable dans les théories de l'Arithmétique supérieure ; et d'ailleurs, il a été accepté depuis Gauss par tous ceux qui ont fait faire quelques progrès

à la Théorie des nombres. De plus, dans notre méthode de calcul symbolique, nous avons employé le signe ≏; on ne doit pas considérer ce symbole autrement que le signe = de l'égalité; mais nous avons pris cette forme spéciale pour indiquer au lecteur qu'il faut faire le développement des deux membres de la formule symbolique, avant d'écrire leur égalité, ou leur identité.

Tels sont les principaux points sur lesquels nous croyons devoir appeler l'attention. Nous savons bien que certaines des théories exposées paraîtront parfois trop longues et parfois trop concises; aussi nous regrettons de n'avoir pu faire subir à cet ouvrage l'épreuve d'un enseignement public. Cependant nous espérons l'améliorer dans une édition ultérieure, et nous invitons tous nos lecteurs à vouloir bien nous soumettre les observations, corrections et additions, que son étude pourra leur suggérer.

INTRODUCTION.

« Lexque datur numeris magnorum horrenda laborum
(OVIDE, *Metam.*, liv. VII).

Dès son apparition sur la terre, l'homme imagine le calcul pour distinguer, pour compter les objets qu'il échange ou dont il a besoin. Puisqu'il n'a ni papier, ni crayon, il compte en faisant des marques ou des stries sur les troncs d'arbres, sur les os des animaux, ou bien encore il assemble des cailloux (d'où vient le mot *calcul*), qui lui rappellent le nombre des objets qu'il a considérés. On retrouve, dans les cavernes de l'époque primitive, des os striés régulièrement, comme la taille de la boulangère, dont l'origine et le but sont incontestables. Ils servaient à compter, par le procédé le plus élémentaire qui représente l'idée même de la formation des nombres, par l'addition successive de l'unité.

Plus de trente-cinq siècles avant notre ère, les Chinois se servaient de boules pour représenter les nombres. Ils employaient, dans le commerce et dans les affaires, de petites cordes à nœuds dont chacune avait sa signification particulière. Elles sont représentées dans deux tables que les Chinois appellent *Ho-tou* et *Lo-chou* (¹), et qui sont, de deux façons différentes, la figuration des neuf premiers nombres, au moyen de boules.

(¹) « Les premières colonies qui vinrent habiter le Se Tchuen n'avaient, pour toute littérature, que quelques abaques arithmétiques faits avec de petites cordes nouées, à l'imitation des chapelets, à globules enfilés, avec quoi ils calculaient et faisaient leurs comptes dans le commerce. Ils les portaient sur eux et s'en servaient quelquefois pour agrafer leurs robes; du reste, n'ayant pas de caractères, ils ne savaient ni lire, ni écrire. » (DUHALDE, *Description de la Chine*

Les anciens Tartares avaient, pour s'entendre, des *khé-mou* ou bâtonnets entaillés d'une manière convenue; ils s'en servaient pour communiquer d'une horde à l'autre. Ces bâtonnets indiquaient, en temps de guerre, le nombre d'hommes et de chevaux que chaque campement devait fournir. Les habitants du Pérou, au temps des Incas, avaient des cordelettes nouées qu'ils appelaient des *Quippos,* et dont on trouve plusieurs échantillons au musée ethnographique du Trocadéro. Elles étaient de différentes couleurs et pouvaient se nouer et s'entrelacer de bien des manières. Le nombre des nœuds, leurs dispositions, leurs enchevêtrements avec des baguettes, leurs situations diverses sur un anneau central en métal, en bois ou en os, permettaient d'exprimer de cette façon une suite assez considérable de nombres.

Ainsi, la première notion du nombre, qui a dû précéder de plusieurs siècles l'alphabet et l'écriture, n'est qu'une simple question d'ordre ou de *numérotage.* De là résulte immédiatement l'idée de la suite des nombres entiers et, simultanément, celle de l'*addition.* Au lieu de compter par un, dans la suite naturelle des nombres désignés par des mots convenus, on compte de deux en deux, et l'on distingue les nombres pairs des nombres impairs. Déjà, dans le *Lo-chou,* les nombres *pairs* sont représentés par des boules noires et les nombres *impairs* sont représentés par des boules blanches. Puis l'on compte de trois en trois, de quatre en quatre, ..., et l'on a la notion de l'addition par cette question : Quel est le nombre qui vient un certain nombre de rangs après un autre? Dès lors, les premières propriétés des nombres apparaissent à l'humanité, car l'idée d'addition est indépendante de la continuité, de la grandeur, de la mesure; elle ne dépend que de l'ordre ou du numérotage. C'est qu'en effet « les principes généraux de l'Analyse mathématique ont leur source naturelle dans la simple considération de l'ordre ou de la disposition mutuelle qu'on peut observer actuellement entre plusieurs objets ; ce qui

---

et de la Tartarie chinoise, p. 293; 1735). — Voir, pour plus de détails, notre article de *La Nature* du 1er mars 1890, intitulé *Chinoiserie arithmétique.*

me paraît le plus haut point d'abstraction et de généralité où il soit permis de porter la science » (¹).

C'est ainsi que, parmi les principales propriétés des nombres, on trouve dès le commencement cette proposition que l'on doit considérer comme l'axiome fondamental des Mathématiques : Le nombre est indépendant de l'ordre et des divers groupements de ses unités. Dans le *Lo-chou,* que nous figurons avec des chiffres, au lieu de boules, les neuf premiers nombres

4	9	2
3	5	7
8	1	6

sont rangés sur les neuf cases d'un carré, et la somme des nombres renfermés dans une même ligne, dans une même colonne, ou dans chacune des deux diagonales, est constamment égale à quinze. Et pourtant cette figure, qui représentait peut-être une boîte portative de poids, dans laquelle on avait cherché et trouvé l'équilibre, et que l'on appelle actuellement un *carré magique,* doit être considérée comme le plus ancien document de l'Arithmétique, puisqu'elle renferme quelques-unes des propriétés élémentaires des nombres.

Les échanges commerciaux ont donné naissance à la *soustraction,* opération inverse de l'addition, qui revient à ceci : Quel est le nombre qui se trouve un certain nombre de rangs avant un autre? Mais, dans cette opération, il se présente parfois une sorte d'impossibilité; c'est lorsqu'il s'agit de retrancher d'un certain nombre un autre plus grand, plus éloigné dans la série des nombres. De là, dans le commerce, ces distinctions du débit et du

(¹) POINSOT, *Introduction à la Théorie des nombres,* p. 2 du Mémoire, dans le *Journal de Liouville* (t. X, 1845).

crédit, de l'actif et du passif, du doit et de l'avoir. Dans la science pure, cette impossibilité disparaît en donnant des appellations et des signes aux résultats, et l'introduction des *nombres positifs* et des *nombres négatifs,* toute naturelle, se fait d'elle-même. D'abord, si l'on retranche un nombre d'un nombre égal, on dit zéro, et *zéro* devient un nombre entier qui représente l'origine de tous les nombres; puis, après avoir numéroté dans un sens, on numérote dans le sens opposé, comme dans l'échelle des thermomètres, et l'on dit *moins un, moins deux,* .... Il n'est pas douteux que cette interprétation de sens ou de direction, même pour les nombres abstraits, était connue dès la plus haute antiquité. Pour justifier cette opinion, il nous suffit d'indiquer la représentation des nombres voisins de cinq, c'est-à-dire quatre et six, représentés par IV et par VI dans la numération des Romains, ou encore celle des nombres IX et XI qui comprennent X. Mais c'est à Descartes que l'on doit l'introduction systématique des nombres négatifs dans les calculs de la Géométrie, de l'Arithmétique et de l'Algèbre, soit que ces nombres se présentent dans les données des problèmes, soit qu'ils se présentent dans les résultats.

La répétition des mêmes affaires commerciales conduit à l'addition des nombres égaux, ou à la *multiplication,* qui n'est qu'une addition abrégée, encore indépendante de l'idée de mesure, de grandeur, de continuité. Pour calculer plus rapidement, on imagine des tables et des appareils de calcul, que l'on appelle *bouliers* et *abaques*. On doit noter la mémorable invention de Fo-chi, premier empereur et législateur de la Chine (3500 ans avant notre ère), pour représenter les nombres jusqu'à soixante-quatre; c'est le *Je-kim* ([1]), boulier formé de six tiges parallèles sur chacune desquelles on peut faire glisser une seule boule. Lorsque la boule est placée au milieu d'une tige, elle représente deux fois le nombre

---

([1]) *Voir* notre article intitulé *Les appareils de calcul et les jeux de combinaisons,* dans la *Revue scientifique* du 4 janvier 1890.

que représenterait une boule sur la tige placée immédiatement au-dessous. En d'autres termes, de la première à la sixième tige, les boules valent

un, deux, quatre, huit, seize, trente-deux,

et le nombre marqué sur le boulier est la somme des nombres représentés par chacune des boules. Mais, pour parvenir à compter des nombres de plus en plus grands, et, par exemple, pour dénombrer les étoiles du ciel, les habitants d'une ville ou d'une contrée, il fallut d'abord augmenter le nombre des tiges et employer simultanément plusieurs bouliers. En plaçant quatre boules sur chaque tige, on convenait que les boules situées sur les tiges successives avaient une valeur de cinq en cinq fois plus grande; avec neuf boules, il était convenu que chaque tige servait à représenter des nombres de dix en dix fois plus grands. Telle est l'origine du boulier chinois nommé *souan-pan*, du boulier russe nommé *schtote* et des diverses transformations de ces appareils dont on se servait couramment en Europe, au XIVe siècle, dans les calculs de la *Banque des argentiers*. Les Chinois, les Russes et les peuples de l'Orient se servent encore couramment des bouliers. Le jeu d'anneaux, que l'on appelle *baguenaudier*, d'origine chinoise, doit être considéré comme une transformation du Je-kim et construit plus spécialement pour la classe des lettrés et des mandarins.

L'emploi des bouliers conduit directement à la numération parlée et à la numération écrite; la numération décimale était connue en Chine et aux Indes, dès les temps les plus reculés; elle nous a été transmise par les Arabes, avec leurs chiffres et le *zéro*. On ne doit pas confondre les *abaques* avec les tables de multiplication; dans l'origine, c'étaient des tables en bois, en métal ou en marbre, divisées en compartiments par des lignes transversales; ces compartiments correspondaient aux tiges des bouliers; on y plaçait des pions ou des cailloux, ou l'on y traçait encore des signes sur le sable, le *pulvis eruditus,* dont ils étaient recouverts, comme dans la *Table de Salamine,* ou l'abaque de Boëce. « Le

système de numération décrit par Boëce est identique, quant aux principes, à notre Arithmétique actuelle et n'en diffère, en pratique, qu'en ce seul point, qu'on faisait usage d'un *Tableau à colonnes,* pour indiquer les différents ordres d'unités décuples, ce qui permettait de marquer par une *place vide* l'absence d'un nombre, que nous marquons aujourd'hui par un signe figuré, c'est-à-dire, en d'autres termes que, dans ce système, le zéro était une place vide » ([1]). — Mais pendant leurs vingt siècles d'existence les Romains n'ont pas connu l'emploi du zéro. Ils n'avaient pour numération que le système défectueux qu'ils nous ont transmis; par suite, ils ignorèrent l'Arithmétique et la Géométrie. Ils ont dédaigné les connaissances si subtiles, si idéales des Grecs qu'ils avaient conquis; ils ont brûlé les écrits d'Archimède. Leurs mathématiciens étaient des esclaves, les *Calculatores,* et leur bagage scientifique se réduit aux médiocres travaux des *Agrimensores* et des *Gromatici* de la décadence.

Les questions des partages et des héritages, que l'on rencontre continuellement dans les ouvrages des auteurs arabes, avaient donné naissance, d'une part, à la division et aux nombres fractionnaires; d'autre part, à la Géométrie, par l'évaluation des surfaces et des volumes. Dès les temps les plus reculés, les Hindous figuraient les nombres par des briquettes de bois ou d'argile, en forme de parallélépipèdes rectangles de même hauteur, et dont la longueur et la largeur étaient des multiples de la hauteur. C'est en tenant compte des indications puisées dans les ouvrages d'Aryabhatta que nous avons pu reconstituer la *Table de multiplication des Indiens,* dont on trouvera un exemplaire dans la collection des machines à calcul que nous avons réunies au Conservatoire des Arts et Métiers. Au moyen de cette Table, on peut démontrer la plupart des théorèmes concernant la mesure des surfaces et des volumes, ainsi que les formules sur la somme des premiers nom-

---

([1]) Chasles, *Explication des Traites de l'*Abacus *et, particulièrement, du Traité de* Gerbert (*Comptes rendus de l'Académie des Sciences;* Paris, 1843).

bres entiers, triangulaires, carrés, cubes, etc. (*voir* Chap. V et XIV). Mais, pour parvenir à la sommation des puissances numériques de tous les degrés, il fallait inventer des nouveaux procédés de calcul dont on trouve la base dans le *Triangle arithmétique* qui était connu des mandarins chinois; mais c'est surtout à FERMAT et à PASCAL qu'il faut attribuer le développement de cette admirable méthode de calcul au moyen de laquelle ils sont parvenus à résoudre les problèmes des combinaisons et du Calcul des probabilités, ainsi qu'à établir les formules fondamentales du Calcul des sommes, du Calcul différentiel et du Calcul intégral.

PYTHAGORE (né v. 580 av. J.-C.) était allé s'instruire en Égypte et dans les Indes, avant de fonder en Italie l'école pythagoricienne. On appelle *Table de Pythagore* la table de multiplication des premiers nombres; l'observation de la table montre, en plus de la symétrie, que son intérieur ne renferme pas tous les nombres, mais ne contient que ceux qui sont le produit de deux autres; de là, la distinction des entiers en *nombres premiers* et en *nombres composés* et la théorie des *diviseurs* et des *multiples*. Dans le VII[e] Livre des *Éléments de Géométrie*, EUCLIDE (v. 285 av. J.-C.) en a exposé les premiers principes avec l'élégance et la rigueur ordinaires aux anciens; c'est à EUCLIDE que l'on doit cette proposition : *La suite des nombres premiers est illimitée.* On lui doit encore l'idée des *nombres parfaits, abondants, déficients, aliquotaires,* c'est-à-dire des entiers qui sont égaux à la somme de leurs parties aliquotes, ou plus petits ou plus grands, ou égaux à une fraction donnée de cette somme. Cette recherche a été continuée par FERMAT, DESCARTES, FRÉNICLE, EULER, et reprise de nos jours; mais, malgré les efforts des savants les plus illustres, elle a fait peu de progrès depuis vingt siècles; on ne connaît actuellement que neuf nombres parfaits pairs et l'on ne sait pas s'il existe des nombres impairs qui soient parfaits.

C'est à PYTHAGORE et à ses disciples que l'on attribue les premières notions de la doctrine des nombres incommensurables. On doit noter surtout une démonstration de l'incommensurabilité du rapport de la diagonale d'un carré à son côté; c'est une figuration

l.

géométrique du développement de $\sqrt{2}$ par la méthode dite des *fractions continues*, retrouvée au XVI[e] siècle par CATALDI, mais qui était bien connue des géomètres indiens sous une forme plus élégante, plus systématique. Pour la résolution des problèmes, ils avaient imaginé l'analyse indéterminée du premier degré et du second degré; on en retrouve des exemples sur les papyrus et les obélisques des Égyptiens.

L'extraction de la racine carrée d'un nombre entier A ayant été reconnue impossible, en démontrant qu'on ne pouvait résoudre en nombres entiers l'équation

$$x^2 - Ay^2 = 0,$$

ils avaient remplacé celle-ci par l'équation, dite de PELL,

$$x^2 - Ay^2 = \pm 1.$$

Les ouvrages de BRAHMEGUPTA et de BHASCARA ACHARYA donnent la manière de déduire, d'une seule solution, toutes les autres solutions entières d'une équation indéterminée du second degré à deux inconnues, et cette analyse, que nous attribuons à EULER et à LAGRANGE, était connue aux Indes depuis plus de dix siècles! Mais nous devons rappeler surtout l'admirable et rapide procédé d'extraction de la racine carrée que nous expliquerons sur $\sqrt{2}$. On considère 2 comme le produit des nombres 1 et 2; on en prend la moyenne arithmétique et la moyenne harmonique, et l'on obtient les deux nombres $\frac{3}{2}$ et $\frac{4}{3}$ dont le produit est égal à 2; en répétant sur ces deux nombres l'application du procédé, on obtient les deux nombres $\frac{17}{12}$ et $\frac{24}{17}$ de produit 2, puis les deux nombres $\frac{577}{408}$ et $\frac{816}{577}$, et ainsi de suite. On arrive ainsi rapidement à deux suites de nombres : les moyennes arithmétiques et les moyennes harmoniques. On démontre facilement par le calcul ou par une figure géométrique que les premières vont en décroissant, en surpassant $\sqrt{2}$; que les secondes vont en croissant sans dépasser $\sqrt{2}$, et que la différence des deux moyennes du même rang décroît avec une très grande rapidité.

En effet, ce procédé revient à l'emploi simultané des fractions continues et du calcul par logarithmes, puisque l'on calcule les réduites du développement de $\sqrt{2}$ dont les indices vont en progression géométrique; et ainsi, pour écrire et non pour calculer les deux moyennes dont le rang est 64, il faudrait, par ce procédé de Baudhayana et d'Apastamba, plus de *deux cent millions de siècles!*

Nous avons cherché pendant longtemps l'extension de ce procédé aux racines cubique, biquadratique, etc.; le lecteur en trouvera les premières notions dans l'*Addition* X. Nous en avons déduit un procédé de généralisation indéfinie des fractions continues, en supprimant, comme il fallait s'y attendre, l'algorithme incommode et défectueux de Cataldi et de Brouncker, et en nous servant de la théorie des substitutions linéaires.

C'est encore à Pythagore, qui l'avait peut-être empruntée aux Indiens, que l'on attribue l'idée des *triangles rectangles numériques,* c'est-à-dire ceux dont les côtés sont des nombres entiers tels que 3, 4, 5. En généralisant la méthode de Pythagore, qui repose sur le théorème du carré de l'hypoténuse, on obtient la formule suivante

$$(r^2-s^2)^2+(2rs)^2=(r^2+s^2)^2,$$

que Proclus a attribuée à Platon (430-347 av. J.-C.). Nous démontrerons, dans le second volume, quo cette formule renferme sans exception tous les triangles rectangles *primitifs* (c'est-à-dire ceux dont les côtés sont des nombres premiers entre eux), quand on y remplace r et s par des nombres premiers entre eux, mais de parité différente. Cette étude a été développée surtout par Diophante, à l'École d'Alexandrie, puis par les Indiens et par les Arabes. Dès le IVe siècle de notre ère, le géomètre indien Brahmegupta donnait des formules plus générales pour le triangle et pour le quadrilatère inscriptible dont les côtés, les diagonales, les rayons des cercles tangents à trois côtés, la surface, etc., sont des nombres entiers; et l'on peut dire que la science arithmé-

tique principale des Arabes d'Orient et d'Occident, jusqu'au XVI[e] siècle, fût consacrée à l'étude de ces figures et à leur classification.

Nous présenterons ici quelques développements sur des théories qui paraissent étrangères à notre sujet, afin de montrer l'extrême importance de l'identité de PLATON et, par suite, même en ce cas particulier, le rôle universel de l'Arithmétique. Si l'on pose

$$\operatorname{tang}\frac{\varphi}{2} = \frac{s}{r},$$

on a, comme l'on sait,

$$\cos\varphi = \frac{r^2 - s^2}{r^2 + s^2}, \qquad \sin\varphi = \frac{2rs}{r^2 + s^2}, \qquad \operatorname{tang}\varphi = \frac{2rs}{r^2 - s^2};$$

on peut donc exprimer toutes les lignes trigonométriques d'un arc φ et de tous ses multiples par des fonctions rationnelles de la tangente du demi-arc, c'est-à-dire de r et de s. Et ainsi toute la Trigonométrie rectiligne n'est que le développement de calculs qui reposent sur cette identité. — On la retrouve continuellement dans la théorie analytique des sections coniques, pour les équations

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \qquad x^2 + y^2 = e^2\gamma^2, \qquad ax^2 + by^2 + cz^2 = 0,$$

soit que l'on rapporte ces courbes à deux systèmes de diamètres conjugués, soit à un foyer, soit à un triangle autopolaire. Par suite encore, cette identité se reproduit constamment dans les théories des cônes du second ordre et des coniques sphériques.

L'identité de PLATON généralisée conduit à la formule

$$(r^2 + s^2)(r_1^2 + s_1^2) = (rr_1 - ss_1)^2 + (rs_1 + r_1 s)^2;$$

celle-ci permet de résoudre le problème de trouver des triangles rectangles numériques dont l'hypoténuse est égale au produit des hypoténuses de deux autres; elle est due aux géomètres

indiens et se trouve dans le *Liber quadratorum* de FIBONACCI (1202). En supposant $r = r_1$ et $s = s_1$, on retombe sur l'identité précédente. Cette formule exprime que le produit d'une somme de deux carrés par une somme de deux carrés est égale à une somme de deux carrés; on dit encore que le module du produit de deux nombres imaginaires est égal au produit des modules. On démontre que toutes les solutions entières de l'équation indéterminée

$$x^2 + y^2 = z^n$$

sont données par la formule

$$z = (r + si)^n = x + yi \qquad (\text{mod } i^2 + 1),$$

et ainsi la théorie des nombres imaginaires, la formule de MOIVRE, etc., découlent encore de l'identité de PLATON. Celle-ci permet encore de faire disparaître l'irrationnalité apparente de nombreuses formules contenant le radical $\sqrt[n]{x^2 + y^2}$; pour faire disparaître le radical on exprime x et y en fonction rationnelle de r et de s, par l'équation précédente. Plus généralement, on peut remplacer l'expression $(x^2 + y^2)$ placée sous le radical, par une forme quadratique binaire quelconque $(ax^2 + 2bxy + cy^2)$. Ces transformations importantes trouvent continuellement leur emploi dans la théorie des équations, dans celle des courbes algébriques et dans le Calcul intégral. Lorsque la quantité placée sous le signe d'intégration est une fonction rationnelle de la variable x et des radicaux $\sqrt{x - a}$, $\sqrt{x - b}$, ou encore une fonction rationnelle de la variable x et du radical $\sqrt{a + bx + cx^2}$, on ramène le problème, par l'identité de PLATON, à l'intégration d'une fonction rationnelle d'une autre variable. Il en est de même lorsque le signe d'intégration renferme une fonction rationnelle des lignes trigonométriques des multiples et des sous-multiples de la variable.

« L'*Arithmétique* de DIOPHANTE, qui est entièrement consacrée aux problèmes indéterminés, contient un grand nombre de

questions qui, par leur difficulté et la subtilité des artifices, donnent une grande idée du génie et de la pénétration de l'auteur, surtout quand on considère le peu de ressources qu'il pouvait employer; mais, comme ces problèmes demandent plutôt de l'adresse et des procédés ingénieux que des principes difficiles, et qu'en outre ils sont trop particuliers et conduisent rarement à des conclusions générales, cet ouvrage semble plutôt avoir fait époque dans l'histoire des Mathématiques, parce qu'il fixe les premiers vestiges de l'Algèbre, qu'avoir enrichi l'Arithmétique transcendante par de nouvelles découvertes. La science est bien plus redevable aux modernes, parmi lesquels peu d'hommes, à la vérité, mais tous dignes d'une gloire immortelle, FERMAT, EULER, LAGRANGE, LEGENDRE (et un petit nombre d'autres), ont ouvert l'entrée de cette science divine et ont découvert la mine inépuisable de richesses qu'elle renferme » (¹).

Cependant l'ouvrage de DIOPHANTE contient, en germe, la plupart des questions de notre science moderne. Dans un mémoire adressé, en 1770, à l'Académie des Sciences de Berlin, LAGRANGE s'exprime ainsi : « C'est un théorème connu depuis longtemps que *tout nombre entier non carré peut toujours se décomposer en deux, ou trois ou quatre carrés entiers,* mais personne, que je sache, n'en a encore donné la démonstration. M. BACHET DE MÉZIRIAC est le premier qui ait fait mention de ce théorème; il paraît qu'il y a été conduit par la question 31 du IVe Livre de DIOPHANTE, où le théorème dont nous parlons est en quelque sorte tacitement supposé; mais M. BACHET s'est contenté de s'assurer de la vérité de ce théorème par induction, en examinant successivement tous les nombres entiers de 1 jusqu'à 325; et quant à la démonstration générale, il avoue qu'il n'avait pas encore pu y parvenir ». C'est en recherchant la démonstration de ce théorème, en procédant du simple au composé, en déterminant quels sont les nombres, qui sont égaux à une somme de deux carrés, d'un carré

(¹) GAUSS, Préface des *Disquisitiones arithmeticæ*, d'après la traduction de POULLET-DELISLE; Paris, 1807.

et du double ou du triple d'un autre carré, que FERMAT parvint à l'énoncé de nombreux théorèmes sur les nombres premiers qui peuvent être représentés par les formes

$$x^2+y^2, \quad x^2+2y^2, \quad x^2+3y^2, \quad \ldots;$$

tels sont les premiers jalons posés dans le champ immense de la théorie des résidus et des formes quadratiques.

En généralisant l'équation donnée par le carré de l'hypoténuse, FERMAT énonce et démontre ce théorème que la somme ou la différence de deux bicarrés n'est jamais un carré, ou, en d'autres termes, qu'on ne peut trouver des nombres entiers ou fractionnaires qui vérifient l'équation

$$x^4 \pm y^4 = z^2;$$

puis il écrit sur une page de son exemplaire de DIOPHANTE l'énoncé d'un théorème, dont il assure avoir la démonstration, mais l'exiguïté de la marge ne saurait la contenir.

Cette proposition connue habituellement, sous le nom de *dernier théorème de Fermat,* s'énonce ainsi : *Il est impossible de résoudre, en nombres entiers ou fractionnaires, l'équation indéterminée*

$$x^p \pm y^p = z^p,$$

dans laquelle p désigne un nombre entier plus grand que 2. Pour $p=3$, le théorème, énoncé avant FERMAT par les algébristes marocains, a été démontré par EULER. Puis LEGENDRE le démontra pour $p=10$, LAMÉ pour $p=7$, LEJEUNE-DIRICHLET dans le cas de $p=5$; enfin M. KUMMER, pour tous les exposants pairs et pour un grand nombre d'exposants premiers, mais beaucoup échappent encore à son analyse. Parmi les plus grands mathématiciens qui, depuis plus de deux siècles, ont aussi recherché vainement la solution de ce problème, qui semble jeté comme un perpétuel défi à l'intelligence humaine, nous signalerons encore les essais intéressants de SOPHIE GERMAIN, d'ABEL, de LIOUVILLE et de LEBESGUE. Et GAUSS lui-même s'en est occupé très longtemps, bien qu'il n'y

fasse aucune allusion dans ses *Disquisitiones,* et qu'il ait écrit que l'Analyse indéterminée était distincte de la Théorie des nombres. Nous en donnerons une preuve irréfutable; c'est la VIIe section de son ouvrage, la plus belle, la dernière, dans laquelle il transforme de tant de manières le quotient de $(x^p - y^p)$ par $(x - y)$; c'est par là qu'il rencontre au détour sa célèbre proposition sur la division de la circonférence en parties égales.

Bachet, dans son Commentaire sur l'Arithmétique de Diophante, pose encore ce problème de trouver deux nombres entiers ou fractionnaires dont la somme ou la différence des cubes soit égale à la somme ou à la différence des cubes de deux nombres donnés, ce qui revient à la résolution de l'équation indéterminée du troisième degré

$$(1) \qquad x^3 \pm y^3 = A z^3,$$

en nombres entiers. Alors il y a lieu de rechercher dans quels cas cette équation est possible ou impossible, pour les valeurs données de A et, dans le cas de possibilité, de trouver toutes les solutions de l'équation. Euler et Legendre ont démontré que l'équation est impossible lorsque A est égal à 1, 2, 3, 4, 5, 18 et 36; mais Legendre s'est trompé pour le cas de $A = 6$, car nous avons démontré le théorème suivant, dans l'*American Journal* (t. II) et dans le *Bulletin de la Société mathématique* (t. VIII) : *Pour que l'équation* (1) *soit vérifiée par des valeurs entières de* A, x, y, z, *il faut et il suffit que* A *soit de la forme* $\lambda\mu(\lambda+\mu)\nu^3$. Pour $\lambda = 1$, $\mu = 2$, $\nu = 1$, on trouve $A = 6$ et en particulier la solution $x = 17$, $y = 37$, $z = 21$, qui avait échappé à l'attention de Legendre. Nous devons encore citer ici les beaux théorèmes de M. Sylvester et du R. P. Pépin : *Si* p, p_1 *et* q, q_1 *désignent des nombres premiers des formes respectives* $(18n+5)$ *et* $(18n+11)$, *il est impossible de résoudre l'équation* (1) *lorsque* A *prend les valeurs*

$$p,\ 2p,\ 9p;\quad p^2,\ 4p^2,\ 9p^2;\quad pq,\ p^2q^2;$$
$$q,\ 4q,\ 9q;\quad q^2,\ 2q^2,\ 9q^2;\quad pp_1^2,\ qq_1^2.$$

Lorsque l'on remplace, dans l'équation (1), l'exposant 3 par l'exposant 5, il existe encore de nombreux cas d'impossibilité, pour des formes générales du nombre A qui ont été indiquées par Dirichlet et par Lebesgue. Mais, d'autre part, si l'on revient à cette équation, dans les cas où elle est résoluble, il y a lieu de rechercher toutes les solutions. Fermat, Lagrange et Cauchy ont donné le moyen de déduire d'une première solution une suite indéfinie d'autres solutions par deux procédés qu'il est plus facile d'expliquer par des considérations de Géométrie analytique. Soient (x, y, z) les coordonnées homogènes d'un point P d'une cubique ayant pour équation cartésienne $f(x, y, z) = 0$. Si les coordonnées du point P sont rationnelles, elles fournissent une première solution en nombres entiers de l'équation indéterminée du troisième degré. Si l'on mène la tangente en P, celle-ci rencontre la cubique en un point unique P' dont les coordonnées, encore rationnelles, représentent une autre solution de l'équation, et ainsi de suite; c'est là le procédé de Fermat. Mais la droite PP' rencontre la cubique en un point unique P'' dont les coordonnées sont encore rationnelles; on déduit ainsi de deux solutions une troisième, et ainsi de suite; cela revient au procédé de Lagrange et de Cauchy; alors il s'agit de classer les solutions obtenues par l'application successive des deux procédés. Cette classification s'obtient par une admirable théorie imaginée par M. Sylvester, et qui s'appelle *Résiduation*. Mais il reste à savoir si l'on obtient ainsi toutes les valeurs entières des inconnues; malgré tant d'efforts, la question n'est pas encore résolue, même dans les cas les plus simples. Nous réserverons pour les volumes qui suivront l'indication de méthodes qui peuvent servir à obtenir de nouveaux résultats dans l'Analyse indéterminée cubique et biquadratique, et dans celle des degrés supérieurs.

C'est en généralisant d'une autre manière le théorème de Bachet que Fermat énonce ce théorème : *Tout entier est une somme de trois triangulaires, de quatre carrés, de cinq pentagones, de six hexagones au plus, et ainsi de suite*. La démonstration de ce théorème, cherchée vainement pendant deux siècles,

n'a été obtenue pour la première fois, que par CAUCHY qui a perfectionné le théorème, en modifiant l'énoncé. Mais après toutes ces propositions de FERMAT que l'on considère comme les dernières, il y en a d'autres encore. Nous publierons, à la suite de cet ouvrage, d'après les extraits d'une correspondance et de manuscrits inédits, les énoncés et le commentaire de vingt-deux propositions aussi difficiles, aussi inaccessibles.

Il nous reste à indiquer, dans une revue rapide, les applications utiles et intéressantes de l'Arithmétique. En laissant de côté son rôle universel dans toutes les sciences, sur tout ce qui se compte et se mesure, nous signalerons d'abord l'*Arithmétique sociale* qui s'occupe des calculs de la banque, du commerce et de l'industrie, des assurances, de la statistique, etc. Par la considération du triangle arithmétique, FERMAT et PASCAL ont jeté les premiers fondements du Calcul des probabilités et ses applications aux jeux de hasard et aux jeux de combinaisons. Le jeu du *taquin,* qui obtint naguère un si grand succès, est une figuration intéressante de la distinction des permutations en deux classes et du théorème de BÉZOUT pour définir les signes des termes d'un déterminant; et, d'ailleurs, tout théorème de Géométrie, d'Algèbre ou d'Arithmétique peut donner lieu à l'invention d'un jeu correspondant. La doctrine des combinaisons trouve encore son application directe dans la *Cryptographie,* en imaginant avec CARDAN, PORTA et BACON, des systèmes de correspondance secrète pour la diplomatie et les armées en campagne, ou en cherchant des procédés de déchiffrement comme ceux de VIÈTE et de M. KERCKHOFFS.

Aux divers systèmes de numération se rapportent le *baguenaudier,* qui est une transformation du boulier du système binaire, ainsi que la *Tour d'Hanoï,* que nous avons publiée en 1882, et le jeu indien de *Tchonka-Rouma;* d'ailleurs, on peut imaginer des appareils du même genre pour tous les systèmes de numération. C'est encore à cette théorie qu'il faut rattacher beaucoup de problèmes sur le jeu de dames et le jeu d'échecs; en particulier, nous citerons le problème des reines dont la solution a été donnée par GAUSS pour l'échiquier ordinaire.

Dans la Géométrie de situation, on doit rappeler le problème des *ponts de la Pregel,* traité par EULER, les divers problèmes sur les *réseaux,* les *labyrinthes,* les arbres géométriques et le jeu de dominos; le jeu du *solitaire,* dont la théorie a été ébauchée par LEIBNIZ, le *jeu icosien* d'HAMILTON, etc. Le théorème des quatre couleurs, posé par GUTHRIE et démontré par M. KEMPE, trouve son utile emploi dans la *Cartographie,* pour le coloriage des cartes avec un nombre minimum de couleurs. Nous rappellerons encore les essais de VANDERMONDE sur la Géométrie des tissus à fils curvilignes et les résultats obtenus par M. TAIT, professeur de l'Université d'Édimbourg, dans la *Géométrie des nœuds,* par des considérations difficiles sur la partition des nombres.

La théorie des nombres premiers trouve d'importantes applications dans les diverses dispositions des *tours à fileter;* nous y rattacherons le problème de MONGE, concernant le *battement* d'un jeu de cartes, qui est une figuration intéressante de diverses parties de la théorie des substitutions. C'est par l'application de plusieurs théorèmes de FERMAT que nous avons pu obtenir la classification des armures fondamentales dans la Géométrie du tissage pour les tissus à fils rectilignes. Depuis, c'est par l'emploi de cette méthode que nous avons trouvé une démonstration très simple des théorèmes de LEGENDRE et de JACOBI sur la loi de réciprocité des résidus quadratiques.

Enfin, c'est en cherchant à ranger, à classer les rouages et les engrenages, que deux horlogers sont parvenus à des résultats intéressants et inattendus dans la théorie des nombres. En 1814, FAREY énonce à la *Société philomathique* des propriétés remarquables sur les suites de fractions rangées par ordre de grandeur et dont les termes ne dépassent pas des nombres donnés; ces propriétés ont été démontrées par CAUCHY, amplifiées et perfectionnées par LEJEUNE-DIRICHLET et, tout récemment, par M. SYLVESTER. En 1862, BROCOT, dans un ouvrage sur le *Calcul des rouages par approximation,* a posé, sans s'en douter peut-être, des lois fondamentales pour la formation et la classification des nombres commensurables.

Nous avons inséré, dans ce premier volume, beaucoup de ces applications de l'Arithmétique, soit dans le texte, soit dans les exercices. Les autres trouveront leur place dans une nouvelle édition de nos *Récréations mathématiques,* afin de mettre à profit cette pensée de PASCAL : « Les matières de Géométrie sont si sérieuses d'elles-mêmes, qu'il est avantageux qu'il s'offre quelque occasion pour les rendre un peu divertissantes. »

Paris, juin 1891.

THÉORIE DES NOMBRES.

TOME I.

LIVRE I.

LES NOMBRES ENTIERS.

CHAPITRE I.

ADDITION DES NOMBRES ENTIERS.

1. Les nombres et les signes. — Les nombres sont désignés par des chiffres ou par des lettres; les opérations sont indiquées par des signes; l'égalité ou l'inégalité des résultats d'opérations diverses est indiquée par des signes de relation.

1° *Emploi des chiffres et des lettres.* — Le système de la numération binaire a été imaginé par Fo-Chi, empereur de la Chine (3500 av. J.-C.). La numération décimale vient des Hindous et nous a été transmise par les Arabes. On ignore le nom de l'inventeur du zéro.

Les lettres pour représenter les nombres ont été employées pour la première fois par Viète. Habituellement, les premières lettres de l'alphabet a, b, c, ... désignent les nombres connus, et les dernières x, y, z les nombres inconnus.

2° *Emploi des signes d'opération.*

$\pm$ Les signes $+$ et $-$ de l'addition et de la soustraction sont dus à Widmann (1489) :

$$a \pm b.$$

$. \times$ Le point comme signe de la multiplication est dû à Leibniz

et le signe $\times$ se trouve dans l'ouvrage d'OUGHTRED intitulé : *Clavis mathematica* (1631). Dès 1544, STIEFEL, dans son *Arithmetica integra*, n'employait aucun signe et désignait le produit de deux nombres en les plaçant l'un après l'autre :

$$a.b, \quad a \times b, \quad ab.$$

: Le signe : de la division est dû à LEIBNIZ; la barre de fraction se trouve dans les ouvrages de FIBONACCI (1202); elle est probablement due aux Hindous :

$$a : b, \quad \frac{a}{b}.$$

a^n La notation des exposants se trouve dans l'ouvrage de CHUQUET intitulé : *Triparty en la science des nombres* (1484).

$n!$ Cette notation $n!$ désigne le produit des n premiers nombres entiers, et se lit *factorielle n* : elle a été introduite par KRAMP, en 1808. Les Anglais écrivent $\underline{|n}$.

$a^{n|r}$ Cette notation, imaginée par KRAMP, désigne le produit de n nombres en progression arithmétique commençant à a et de raison r.

$\mathrm{E}\frac{p}{q}$ Cette notation désigne le plus grand nombre entier contenu dans la fraction $\frac{p}{q}$, et se lit *entier de p sur q*.

3° *Emploi des signes de relation.*

$=$ Le signe $=$ de l'égalité est dû à RECORDE (1557). DESCARTES et FERMAT se servaient du signe $\propto$.

$\gtrless$ Les signes $>$ *plus grand que* et $<$ *plus petit que* de l'inégalité ont été imaginés par HARRIOT (1631).

( ) [ ] L'emploi des *parenthèses* ( ) et des *crochets* [ ] a été introduit par ALBERT GIRARD, en 1629. On se sert aussi parfois du *vinculum*, ou d'un trait placé au-dessus d'une expression algébrique pour désigner sa valeur numérique ou son ensemble.

$\equiv$ Le signe $\equiv$ de la congruence a été imaginé par GAUSS. Ainsi $a \equiv b \pmod{m}$, qui se lit *a congru à b pour le module m*, veut dire que $a - b$ est divisible par m. Cette notation est très utile dans l'Arithmétique supérieure.

$\left(\frac{n}{p}\right)$ désigne $+1$ ou -1 suivant que n est ou n'est pas le reste de la division du carré d'un nombre par un nombre premier p, en supposant n non divisible par p. Ce symbole, dû à LEGENDRE, a été généralisé par JACOBI.

2. Addition des nombres entiers. — Formation des nombres entiers. — La suite des nombres entiers est illimitée; en d'autres termes, après tout nombre n, il y en a un autre $(n+1)$.

Formation des nombres pairs et des nombres impairs. Le $n^{\text{ième}}$ nombre pair est $(n+n)$ ou $2n$; le $(n+1)^{\text{ième}}$ nombre impair est $(2n+1)$.

Compter les nombres de trois en trois, de quatre en quatre, etc.

La somme de plusieurs nombres ne dépend pas de l'ordre de ces nombres :

$$a+b+c=c+a+b.$$

Dans la somme de plusieurs nombres, on peut remplacer plusieurs d'entre eux par leur somme, sans changer le total.

Dans la somme de plusieurs nombres, on peut remplacer l'un quelconque d'entre eux par plusieurs autres dont il est la somme.

Table d'addition.

Preuve de l'addition, en changeant l'ordre des termes.

3. Suite de Fibonacci. — Si l'on calcule une suite de nombres commençant par 0 et 1, de telle sorte que chaque terme soit égal à la somme des deux précédents, on forme la suite

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ \ldots;$$

par conséquent, si l'on désigne les différents termes par

$$u_0,\ u_1,\ u_2,\ u_3,\ u_4,\ u_5,\ u_6,\ u_7,\ u_8,\ \ldots,$$

on a la *loi de formation*

$$u_{n+2}=u_{n+1}+u_n.$$

La suite de FIBONACCI possède des propriétés nombreuses fort intéressantes qui seront développées ultérieurement. On en trouve les douze premiers termes dans le *Liber Abbaci* (p. 284) pour la question : *Quot paria coniculorum in uno anno ex uno pario germinentur.* C'est le premier exemple connu des suites récurrentes. Cette même suite a été étu-

[illegible] Lemaire [illegible] [illegible]. Il démontre [illegible] et de la plus grande importance [illegible] de [illegible] faire l'admiration que l'on peut [illegible] la détermination d'une limite supérieure du nombre [illegible] plus grand commun diviseur de deux nombres entiers [illegible] [illegible] — *Recherches nouvelles sur deux* [illegible].

[illegible] nombres de [illegible] arithmétique supérieure [illegible].

[illegible] *la somme des premiers termes* [illegible] *est égale* [illegible] *est arrêtée.* [illegible]

$$[illegible] = u_{n+2}[illegible]$$

[illegible] propriété indiquée [illegible] de n. Supposons [illegible] et pour [illegible]

$$[illegible] = u_{n+2} [illegible]$$

$$[illegible] = u_{n+3} [illegible]$$

par conséquent, en ajoutant ces deux égalités et tenant compte de [illegible]

$$[illegible]$$

cette formule ne diffère [illegible] que par le changement de n en $(n-1)$, puisque u_1 [illegible]. Donc le théorème est démontré.

Ce procédé de démonstration est d'une très grande importance dans l'étude de l'Arithmétique; très souvent l'observation et l'induction ont permis de soupçonner des lois qu'il eût été plus difficile de trouver *a priori*. On se rend compte de l'exactitude des formules par la méthode précédente qui a donné naissance à l'Algèbre moderne par les études de Fermat et de Pascal sur le triangle arithmétique.

Exemple I. — On a, pour la somme des termes de rang pair et pour celle des termes de rang impair, les formules

$$u_1 + u_3 + u_5 + \ldots + u_{2n+1} = u_{2n+2},$$
$$1 + u_2 + u_4 + \ldots + u_{2n} \quad = u_{2n+1}.$$

4. Triangle arithmétique de Pascal. — Le Tableau suivant contient les dix premières lignes du triangle arithmétique.

Fig. 1.

C	0	1	2	3	4	5	6	7	8	9	q
0	1	.	.	.	.	.	.	.	.	.	.
1	1	1	.	.	.	.	.	.	.	.	.
2	1	2	1	.	.	.	.	.	.	.	.
3	1	3	3	1	.	.	.	.	.	.	.
4	1	4	6	4	1	.	.	.	.	.	.
5	1	5	10	10	5	1	.	.	.	.	.
6	1	6	15	20	15	6	1	.	.	.	.
7	1	7	21	35	35	21	7	1	.	.	.
8	1	8	28	56	70	56	28	8	1	.	.
9	1	9	36	84	126	126	84	36	9	1	.
	.	.	.	.	.	.	.	.	.	.	.
p											

Triangle de Pascal.

Par définition, on forme les termes de chaque ligne au moyen des termes de la ligne précédente par cette *loi de formation : Un nombre quelconque du Tableau est égal au nombre placé au-dessus de lui, augmenté du nombre qui précède celui-ci dans la même ligne.*

Pour désigner les différents termes du triangle arithmétique, on numérote les lignes en descendant à partir de 0, et les colonnes successives de gauche à droite, à partir de 0; le terme contenu dans la ligne de rang p et dans la colonne de rang q est indiqué par C_p^q. Avec cette notation, la loi de formation du triangle s'écrit

$$C_{p+1}^{q+1} = C_p^{q+1} + C_p^q.$$

Par hypothèse, on a $C_p^0 = 1$, pour toute valeur entière de p, et même pour $p = 0$. On aperçoit d'ailleurs immédiatement que le

nombre des termes de chaque ligne augmente continuellement de 1 : on peut supposer le tableau indéfiniment allongé dans le sens $Cq \rightarrow$, et l'on posera, par convention,

$$C_p^q = 0,$$

pour tout entier q plus grand que p.

Il résulte immédiatement de la loi de formation que, si l'on représente par

(A) 1, a, b, ..., b, a, 1

une ligne quelconque du triangle, la suivante sera

(B) 1, $1+a$, $a+b$, ..., $b+a$, $a+1$, 1 ;

par conséquent, *dans une ligne quelconque du triangle arithmétique, les termes à égale distance des extrêmes sont égaux.* D'autre part, la ligne (B) du triangle contient deux fois tous les termes de la ligne (A) qui précède ; *la somme des termes d'une ligne du triangle arithmétique est le double de la somme des termes de la ligne précédente :* on a donc la formule

$$1 + C_p^1 + C_p^2 + \ldots + C_p^p = 2^p.$$

Un nombre quelconque du triangle est égal à la somme de tous les termes placés au-dessus de lui dans la colonne précédente.

En effet, considérons, par exemple, le terme $C_9^4 = 126$; on a, d'après la loi de formation, les égalités ci-dessous dont il suffit de faire la somme, en supprimant les nombres égaux dans les deux membres de l'égalité obtenue

$$\begin{aligned}
126 &= 70 + 56\\
70 &= 35 + 35\\
35 &= 15 + 20\\
15 &= 5 + 10\\
5 &= 1 + 4\\
\hline
126 &= 56 + 35 + 20 + 10 + 4 + 1.
\end{aligned}$$

Un nombre quelconque du triangle est la somme de tous les

nombres d'une diagonale descendante ↘ *aboutissant au-dessus du nombre considéré.* Cette propriété se démontre comme la précédente; ainsi l'on a, par exemple,

$$126 = 70 + 35 + 15 + 5 + 1.$$

Si l'on fait les sommes successives des nombres du triangle qui sont contenus dans les diagonales ascendantes ↗, *on reproduit la suite de* Fibonacci [1].

En effet, si l'on considère les deux diagonales ascendantes et consécutives

.	1,	5,	6,	1.	Total......	13,
1,	6,	10,	4.	.	»	21,

et si l'on fait la somme, dans chaque colonne, on trouve la diagonale suivante :

1,	7,	15,	10,	1.	Total...... 34

Par conséquent, la somme des nombres d'une diagonale ascendante est égale à la somme des nombres renfermés dans les deux diagonales précédentes.

5. **Tableau de sommes.** — Considérons une suite de quantités rangées suivant une première colonne verticale; désignons ces quantités par u_0, u_1, u_2, ... Avec une quantité quelconque, que nous désignerons par Σu_0, nous formerons une seconde colonne à côté de la première, par les égalités

$$(1) \quad \left\{ \begin{aligned} \Sigma u_1 &= u_0 + \Sigma u_0, \\ \Sigma u_2 &= u_1 + \Sigma u_1, \\ \Sigma u_3 &= u_2 + \Sigma u_2, \\ &\dots\dots\dots\dots \\ \Sigma u_{p+1} &= u_p + \Sigma u_p. \end{aligned} \right.$$

Avec une seconde quantité que nous désignerons par $\Sigma^2 u_0$, l'indice de Σ désignant une nouvelle colonne, nous calculerons la troisième colonne par la loi de formation

$$(2) \quad \Sigma^2 u_{p+1} = \Sigma u_p + \Sigma^2 u_p;$$

[1] Binet, *Sur le dénombrement des combinaisons discontigües* (*Comptes rendus*, t. XVII).

c'est-à-dire que nous déduisons la troisième colonne de la seconde, de la même manière que nous avons déduit la seconde de la première. Par conséquent, avec les deux suites limitées ou illimitées

$$\begin{array}{lllll} u_0 & u_1 & u_2 & u_3 & \ldots, \\ u_0 & \Sigma^1 u_0 & \Sigma^2 u_0 & \Sigma^3 u_0 & \ldots, \end{array}$$

on forme un Tableau de sommes dans lequel l'indice des Σ désigne le rang de la colonne et celui des u le rang de la ligne (*fig.* 2), par la loi générale de formation

$$\Sigma^{q+1} u_{p+1} = \Sigma^q u_p + \Sigma^{q+1} u_p.$$

Fig. 2.

O — Σ

u_0	Σu_0	$\Sigma^2 u_0$	$\Sigma^3 u_0$	$\Sigma^4 u_0$	...
u_1	Σu_1	$\Sigma^2 u_1$	$\Sigma^3 u_1$	$\Sigma^4 u_1$	...
u_2	Σu_2	$\Sigma^2 u_2$	$\Sigma^3 u_2$	$\Sigma^4 u_2$	...
u_3	Σu_3	$\Sigma^2 u_3$	$\Sigma^3 u_3$	$\Sigma^4 u_3$	...
u_4	Σu_4	$\Sigma^2 u_4$	$\Sigma^3 u_4$	$\Sigma^4 u_4$	...
..	....	....	....	....	...
..	....	....	....	....	...
..	....	....	....	....	...

u

Tableau de sommes.

En d'autres termes, le Tableau possède par définition la propriété suivante : *Un nombre quelconque, à l'intérieur d'un Tableau de sommes, est égal au terme placé au-dessus de lui, augmenté du terme qui précède celui-ci.*

Lorsque les termes de la première colonne sont égaux à 1, et ceux de la première ligne qui suivent u_0 à zéro, on retrouve le triangle arithmétique. Comme le triangle, ce Tableau devenu rectangle possède des propriétés analogues. Si l'on ajoute les égalités (1) en supprimant les quantités égales de part et d'autre, on a

$$\Sigma u_{p+1} = \Sigma u_0 + u_0 + u_1 + u_2 + \ldots + u_p.$$

De même, si l'on ajoute les égalités obtenues en remplaçant p par 0, 1, 2, ..., p, dans l'égalité (2), on trouve

$$\Sigma^2 u_{p+1} = \Sigma^2 u_0 + \Sigma u_0 + \Sigma u_1 + \Sigma u_2 + \ldots + \Sigma u_p;$$

et de même, en général,

$$\Sigma^{q+1} u_{p+1} = \Sigma^{q+1} u_0 + \Sigma^q u_0 + \Sigma^q u_1 + \ldots + \Sigma^q u_p.$$

Cette relation subsiste lorsque l'on augmente tous les indices des Σ d'un entier quelconque; d'ailleurs, on suppose par convention $\Sigma^0 u_p = u_p$, pour l'indice zéro des Σ. De même, puisque l'on peut supposer que le Tableau commence à une ligne quelconque, on peut augmenter tous les indices des u d'un entier quelconque α. On a donc la formule générale

$$(3) \qquad \Sigma^{q+1} u_{p+\alpha+1} = \Sigma^{q+1} u_\alpha + \Sigma^q u_\alpha + \Sigma^q u_{\alpha+1} + \ldots + \Sigma^q u_{\alpha+p}.$$

Par conséquent : *Tout nombre de l'intérieur d'un Tableau de sommes est égal à la somme d'un nombre quelconque de termes consécutifs placés immédiatement au-dessus de lui dans la colonne précédente, augmentée du terme qui suit le plus élevé de celle-ci.*

Reprenons la première des relations (1). En passant à la ligne et à la colonne suivantes, c'est-à-dire en augmentant successivement l'indice de Σ et celui de u d'une unité, on obtient les égalités

$$\begin{aligned}
\Sigma u_1 &= u_0 + \Sigma u_0, \\
\Sigma^2 u_2 &= \Sigma u_1 + \Sigma^2 u_1, \\
\Sigma^3 u_3 &= \Sigma^2 u_2 + \Sigma^3 u_2, \\
&\ldots\ldots\ldots\ldots\ldots\ldots, \\
\Sigma^{p+1} u_{p+1} &= \Sigma^p u_p + \Sigma^{p+1} u_p.
\end{aligned}$$

En les ajoutant et en supprimant les parties égales dans les deux membres, on a

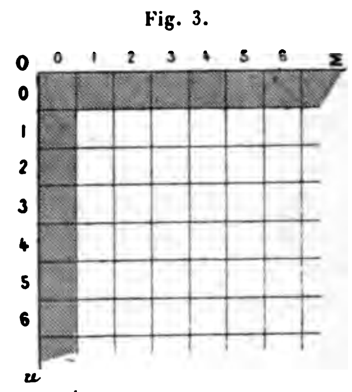
$$(4) \qquad \Sigma^{p+1} u_{p+1} = u_0 + \Sigma u_0 + \Sigma^2 u_1 + \ldots + \Sigma^{p+1} u_p;$$

cette relation subsiste dans toute l'étendue de la Table, et l'on peut augmenter d'un entier quelconque α l'indice des u. On trouve ainsi la somme des nombres consécutifs d'une *diagonale descendante* ↘, tandis que la formule (3) donne la somme de nombres consécutifs d'une colonne ↓.

Si l'on suppose les nombres du Tableau placés sur les cases

d'un échiquier fini ou indéfini $u O \Sigma$, la connaissance de deux suites de nombres placés dans les cases grises (*fig.* 3) permet de remplir toutes les cases de l'échiquier au moyen de l'opération indiquée par A (*fig.* 4), le nombre contenu dans la case noire étant égal à la somme des nombres contenus dans les deux cases grises supérieures. Cette figure, qui se reproduit dans toute l'étendue de l'échiquier, est la

Fig. 3.

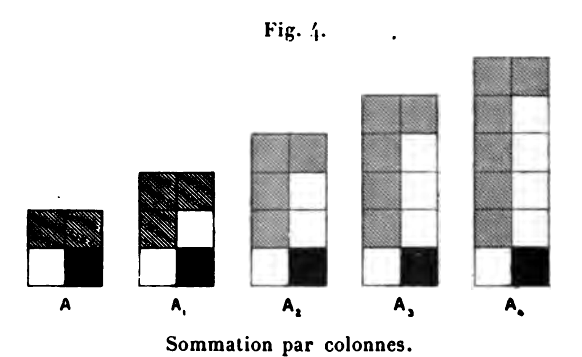


Échiquier arithmétique.

représentation géométrique de la loi de formation du Tableau des sommes.

Si l'on remplace la case grise de droite, dans A (*fig.* 4), par la somme des nombres contenus dans les deux cases de la ligne

Fig. 4.



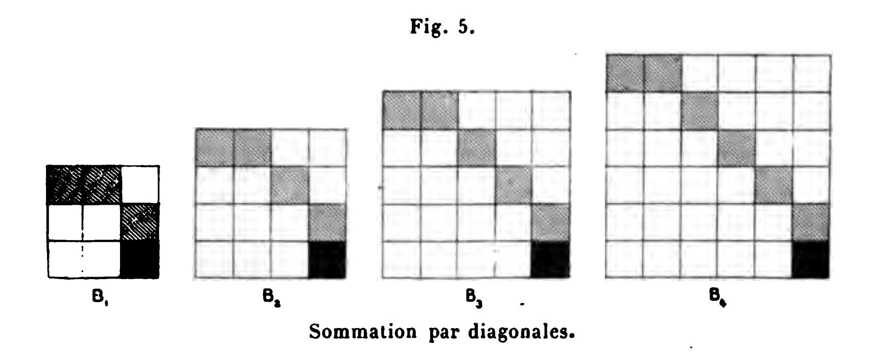
Sommation par colonnes.

précédente, on obtient la *fig.* A_1; puis, en répétant la même opération, on a encore les *fig.* A_2, A_3, A_4, ... Dans chacune

d'elles, le nombre de la case noire est la somme des nombres contenus dans les cases grises.

Au lieu de remplacer la case grise de droite, on peut remplacer celle de gauche, dans A, et l'on obtient $B_1, B_2, B_3, \ldots$ (*fig.* 5), qui correspondent à la seconde propriété du Tableau des sommes.

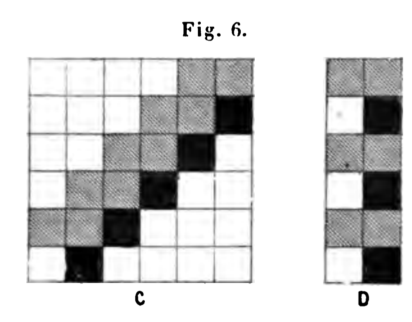
Fig. 5.



Sommation par diagonales.

La juxtaposition d'un nombre quelconque de ces figures donne autant de relations que l'on veut, et ainsi dans C et D (*fig.* 6); la somme des nombres renfermés dans les cases noires est égale à celle des nombres contenus dans les cases grises.

Fig. 6.



Sommation par transversales.

La *fig.* C nous montre comment on peut déduire la suite de Fibonacci des diagonales ascendantes du triangle arithmétique.

6. Généralisations du Tableau des sommes et de la suite de Fibonacci. — On peut considérablement amplifier les considéra-

terminer le nombre des manières de lire le mot cabalistique. Le nombre des lectures se calcule par le Tableau (*fig.* 11).

Fig. 11.

				1				
			1	1	1			
		1	2	3	2	1		
	1	3	6	7	6	3	1	
1	4	10	16	19	16	10	4	1
.	.	.	.	.	.	.	.	.

Marches du roi des échecs.

Chacun des nombres du Tableau est égal au nombre placé au-dessus de lui, augmenté des deux nombres voisins; la somme des nombres de chaque ligne est une puissance de 3. D'ailleurs, nous verrons plus loin que le triangle de Pascal représente les coefficients du développement de la puissance $(x+1)^n$ du binôme, et que le Tableau précédent représente les coefficients du développement de $(x^2+x+1)^n$.

Le calcul précédent permet de déterminer successivement le nombre des marches du *Roi au jeu des échecs*, en supposant que le roi avance continuellement d'un rang vers le camp opposé, sur un échiquier illimité, c'est-à-dire en progressant par cases consécutives dans les trois sens ↙ ↓ ↘. Mais, dans le cas d'un échiquier limité, il faut mettre des zéros sur les cases qui correspondraient à l'extérieur de l'échiquier, tout en conservant la même loi de formation.

Exemple III. — De combien de manières un pion du jeu de dames, placé

Fig. 12.

1	1									
1	.	1								
2	1	.	1							
3	.	2	.	1						
6	2	.	3	.	1					
10	.	5	.	4	.	1				
20	5	.	9	.	5	.	1			
35	.	14	.	14	.	6	.	1		
70	14	.	28	.	20	.	7	.	1	
126	.	42	.	48	.	27	.	8	.	1

Marches du pion du jeu de dames.

en un coin du damier, peut-il se rendre sur le bord opposé, c'est-à-dire en progressant par cases consécutives dans l'un des deux sens ↙ et ↘.

On forme un Tableau comme celui du triangle arithmétique, dans lequel chaque nombre du Tableau est égal à la somme des deux nombres de la ligne précédente qui sont les plus rapprochés (*fig.* 12). Si l'on fait la somme des nombres de chaque ligne, ainsi que nous l'avons calculé à gauche de la figure, on trouve pour le damier de 10 cases de côté que le nombre demandé est 126.

En général, si le damier a $2n$ cases de côté, le total de la dernière ligne est égal au nombre C_{2n-1}^{n-1} du triangle de Pascal, et si le damier a $(2n+1)$ cases de côté, le total est égal à C_{2n}^{n}.

Exemple IV. — On trouve dans le tome IV du *Recueil des Machines de l'Académie des Sciences* (1704) la description d'un appareil ingénieux pour opérer automatiquement l'addition et la soustraction, et qui appartient au Conservatoire des Arts et Métiers; c'est l'*Abaque* de PERRAULT. Tout récemment cet appareil a été perfectionné et publié, à Paris, sous le nom d'*Arithmographe* de TRONCET.

CHAPITRE II.

SOUSTRACTION DES NOMBRES ENTIERS.

---

7. Soustraction des nombres entiers. — *Reste, excès* ou *différence.*

La différence de deux nombres ne change pas lorsqu'on les augmente d'une même quantité.

Opération de la soustraction par l'addition. — Preuve de l'opération.

8. Introduction des nombres entiers négatifs. — Convention de DESCARTES. — Signes des segments.

Quelles que soient les positions respectives A, B, C de trois points en ligne droite, on a l'identité

$$AB + BC + CA = 0.$$

Coordonnées des points d'intersection de deux systèmes de droites parallèles. — Coordonnées des cases d'un échiquier fini ou indéfini. — La notation *expressive* des cases de l'échiquier due à VANDERMONDE, et dérivée du système des coordonnées de DESCARTES, s'applique à un très grand nombre de jeux de calcul et de combinaisons, comme les *échecs*, les *dames*, le *solitaire*, etc. Cette méthode, la plus simple, la plus commode, la plus générale, aurait dû être acceptée depuis longtemps.

Deux cases de l'échiquier (x, y) et (x', y') sont sur une même parallèle à la diagonale descendante ↘, si l'on a $x - x' = y - y'$.

Elles sont sur une même parallèle à la diagonale ascendante, si l'on a $x + \varepsilon x' = y - \varepsilon y'$, en désignant par ε un des nombres $+1$ ou -1. Deux cases du damier sont de même couleur, ou de couleurs différentes, si les sommes $x \pm y$ et $x' \pm y'$ sont ou ne sont pas de même parité.

9. Somme algébrique. — La somme algébrique de nombres entiers, positifs ou négatifs, est indépendante de l'ordre des termes.

Pour ajouter plusieurs sommes algébriques, il suffit de les placer les unes à la suite des autres, avec les signes respectifs de chacun de leurs termes.

Pour retrancher une somme algébrique, on l'écrit à la suite, en changeant les signes de tous ses termes.

Dans l'égalité de deux sommes algébriques, on peut faire passer un terme d'un membre dans l'autre en changeant son signe.

Les théorèmes de l'addition s'appliquent aux nombres entiers algébriques, soit que ces nombres proviennent des données, soit qu'ils proviennent des opérations.

10. Inégalités. — Définition et signes. — Valeur absolue d'un nombre négatif.

On peut ajouter ou retrancher une même quantité aux deux membres d'une inégalité.

On peut faire passer un terme d'un membre dans l'autre en changeant son signe.

On peut changer tous les signes des termes d'une inégalité en changeant le signe de l'inégalité.

On peut ajouter membre à membre des inégalités de même sens.

11. Tableau de différences. — Soit une suite de quantités quelconques

$$u_0,\quad u_1,\quad u_2,\quad \ldots,\quad u_i,\quad \ldots.$$

Si l'on retranche chacune d'elles de la suivante, on forme la suite de leurs *différences premières,* que l'on représente par

$$\Delta u_0,\quad \Delta u_1,\quad \Delta u_2,\quad \ldots,\quad \Delta u_n,\quad \ldots,$$

et l'on a, par définition,

$$\Delta u_n = u_{n+1} - u_n.$$

Si l'on opère sur la seconde suite comme sur la première, on forme une troisième suite, les *différences secondes,* que l'on représente par

$$\Delta^2 u_0,\quad \Delta^2 u_1,\quad \Delta^2 u_2,\quad \ldots,\quad \Delta^2 u_n,\quad \ldots,$$

et l'on a, par définition,

$$\Delta^2 u_n = \Delta u_{n+1} - \Delta u_n.$$

En général, on forme les *différences d'ordre* $(p+1)$ de la suite

initiale, au moyen des différences d'ordre p, par la relation

$$\Delta^{p+1} u_n = \Delta^p u_{n+1} - \Delta^p u_n.$$

On construit le Tableau des différences par colonnes, à gauche de la colonne des u; mais, si l'on observe que l'on a

$$\Delta^p u_{n+1} = \Delta^p u_n + \Delta^{p+1} u_n,$$

on voit que les termes du Tableau jouissent de la propriété qui sert de loi de formation au Tableau des sommes (*fig.* 13).

Fig. 13.

Δ ← → O

...	$\Delta^3 u_0$	$\Delta^2 u_0$	Δu_0	u_0
...	$\Delta^3 u_1$	$\Delta^2 u_1$	Δu_1	u_1
...	$\Delta^3 u_2$	$\Delta^2 u_2$	Δu_2	u_2
...	$\Delta^3 u_3$	$\Delta^2 u_3$	Δu_3	u_3
...	...	...	...	. .

u

Tableau de différences.

12. Tableau de sommes et de différences. — On peut accoler le Tableau des différences au Tableau des sommes, en superposant les colonnes des u, et le nouveau Tableau possédera, dans toute son étendue, les propriétés du Tableau des sommes que nous avons représentées par les A, B, C, D (*fig.* 4, 5, 6).

En exprimant ces propriétés par des formules algébriques, on voit que celles-ci subsistent lorsque l'on augmente ou que l'on diminue tous les indices des Σ et des Δ d'une même quantité, en posant conventionnellement

$$\Sigma^{-p} u_n = \Delta^p u_n, \qquad \Sigma^0 u_n = u_n,$$
$$\Delta^{-p} u_n = \Sigma^p u_n, \qquad \Delta^0 u_n = u_n.$$

Si l'on connaît la suite des u pour des indices négatifs, on peut étendre le Tableau indéfiniment dans tous les sens. On progresse par addition vers la droite → ou vers le bas ↓, et par soustraction vers la gauche ← ou vers le haut ↑ (*fig.* 14).

Les formules algébriques, équivalentes aux *fig.* A, B, C, D, subsistent quelles que soient les valeurs positives, nulles ou négatives, des nombres donnés (qui sont renfermés dans les traits forts) lorsque l'on augmente les indices des Σ et des Δ d'une même quantité, ou encore les indices des u d'une quantité quelconque.

Fig. 14.

				u_{-4}				
				u_{-3}				
				u_{-2}				
				u_{-1}				
$\Delta^4 u_0$	$\Delta^3 u_0$	$\Delta^2 u_0$	Δu_0	u_0	Σu_0	$\Sigma^2 u_0$	$\Sigma^3 u_0$	$\Sigma^4 u_0$
				u_1				
				u_2				
				u_3				
				u_4				

Tableau de sommes et différences.

Le Tableau de sommes possède encore des propriétés importantes. Si l'on multiplie tous les termes par un même nombre ou si l'on change les signes de tous les termes, on obtient encore un Tableau de sommes. Plus généralement, si l'on superpose plusieurs Tableaux de sommes, après avoir multiplié respectivement les termes de chacun d'eux par des nombres quelconques, les nombres obtenus en faisant les sommes algébriques dans chaque case forment encore un Tableau de sommes.

13. Sommes alternées. — On appelle *somme alternée* de n quantités positives ou négatives, u_0, u_1, u_2, ..., la somme algébrique de ces quantités prises alternativement avec le signe + et avec le signe —, c'est-à-dire la valeur de

$$u_0 - u_1 + u_2 - u_3 + \ldots.$$

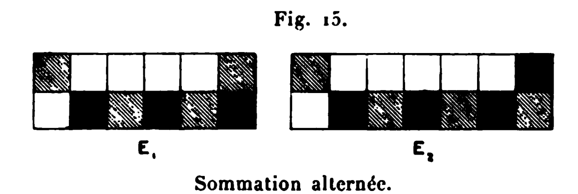
Les propriétés qui résultent des *fig.* A, B, C, D du Chapitre I peuvent s'énoncer de la manière suivante : Si l'on prend avec leurs signes les nombres contenus dans les cases noires et avec les signes contraires les nombres contenus dans les cases grises, la somme algébrique des nombres d'un Tableau de sommes et différences compris sur ces figures est toujours nulle.

Si l'on déplace A (*fig.* 4) horizontalement, en changeant, à chaque déplacement d'un rang, la couleur des cases, on obtient les figures telles que E qui permettent de calculer les *sommes alternées* des termes d'une même ligne (*fig.* 15).

En particulier, pour le triangle de Pascal, la somme alternée d'un nombre quelconque de termes d'une même ligne, à partir du premier, est égale en valeur absolue au terme placé au-dessus du dernier dans la ligne précédente.

Si l'on déplace A (*fig.* 4), parallèlement à la diagonale ascendante ↗, en changeant à chaque déplacement la couleur des cases,

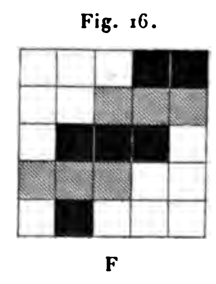
Fig. 15.



Sommation alternée.

on obtient des figures telles que F (*fig.* 16), qui permettent de calculer les sommes alternées des termes d'une parallèle à la diagonale ascendante.

Fig. 16.



Ainsi, pour le triangle de Pascal, la somme alternée de tous les termes d'une diagonale ascendante est égale à la différence des

sommes alternées des termes des deux diagonales précédentes; mais, si l'on calcule les termes de la suite

$$u_0, \quad u_1, \quad u_2, \quad \ldots, \quad u_n, \quad \ldots.$$

par la formule de récurrence

$$u_{n+1} = u_n - u_{n-1},$$

avec les conditions initiales $u_0 = 1$, $u_1 = 1$, on trouve que ces termes se reproduisent périodiquement de six en six, dans l'ordre

$$+1, \quad 0, \quad -1, \quad -1, \quad 0, \quad +1;$$

par conséquent, cette somme alternée est toujours égale à o ou à $+1$ ou à -1.

Remarque. — Telles sont les lois qui régissent l'addition et la soustraction de deux suites de nombres quelconques, l'une représentée par u_n, l'autre par $\Sigma^n u_0$, en donnant à n toutes les valeurs entières. On pourrait les étendre à trois suites et plus.

D'ailleurs il nous semble qu'il n'y en a pas d'autres, si l'on ne veut empiéter sur le domaine de la multiplication, c'est-à-dire de l'addition des nombres égaux. Toutes ces relations s'expriment au moyen des signes + et — de l'addition et de la soustraction, et de leurs symboles extensifs Σ et Δ.

Exemple I. — On a, dans la série de Fibonacci,

$$u_0 - u_1 + u_2 - u_3 + \ldots + \varepsilon u_p = \varepsilon u_{p-1} - 1,$$

ε désignant $+1$ ou -1, suivant que p est pair ou impair.

Exemple II. — Exprimer, au moyen de la notation C_p^q, les propriétés qui résultent des *fig.* A, B, C, E, F pour les termes du triangle de Pascal. On a

$$\text{(A)} \qquad C_{p+1}^{q+1} = C_p^q + C_{p-1}^q + C_{p-2}^q + \ldots + C_q^q,$$

$$\text{(B)} \qquad C_{p+1}^q = C_p^q + C_{p-1}^{q-1} + C_{p-2}^{q-2} + \ldots,$$

$$\text{(C)} \qquad 1 + C_p^1 + C_{p-1}^2 + C_{p-2}^3 + \ldots = u_{p+2},$$

u_{p+2} désignant le terme correspondant de la suite de Fibonacci; puis

$$\text{(F)} \qquad 1 - C_p^1 + C_{p-1}^2 - C_{p-2}^3 + \ldots = 0, \quad \text{ou } +1, \quad \text{ou } -1;$$

$$\text{(E)} \qquad 1 - C_p^1 + C_p^2 - C_p^3 + \ldots + \varepsilon C_p^q = \varepsilon C_{p-1}^q,$$

ε désignant $+1$ ou -1 suivant que q est pair ou impair.

Exemple III. — *Extension du triangle de Pascal.* — On prolonge dans tous les sens le triangle de Pascal, avec la convention $C_p^0 = 1$, pour toutes les valeurs entières de p, positives, nulles ou négatives.

Fig. 17.

.	.	.	1	−4	+10	−20	+35	...
.	.	.	1	−3	+6	−10	+15	...
.	.	.	1	−2	+3	−4	+5	...
.	.	.	1	−1	+1	−1	+1	...
0	0	0	1	0	0	0	0	...
.	.	.	1	1	.	.	.	...
.	.	.	1	2	1	.	.	...
.	.	.	1	3	3	1	.	...
.	.	.	1	4	6	4	1	...
...	...	...	...	...	...	...	...	...

Extension du triangle de Pascal.

On voit qu'il faut supposer $C_p^q = 0$, pour q négatif, ou pour p positif avec $q > p$. De plus, on voit que l'on a, pour p positif,

$$C_{-p}^q = \varepsilon C_{p+q-1}^q,$$

en supposant ε égal à $+1$ ou à -1 suivant que q est pair ou impair. En d'autres termes, si l'on ne tient pas compte des signes, le Tableau de Pascal prolongé vers le haut reproduit le triangle, les lignes remplaçant les diagonales ↘.

14. Des variations de signes. — Dans une suite de nombres positifs ou négatifs, on dit que deux termes consécutifs présentent une *variation* lorsqu'ils sont de signes contraires, et une *permanence* lorsqu'ils ont le même signe.

Si l'on introduit un terme entre deux termes successifs de signes contraires, le nombre des variations ne change pas.

Si l'on introduit un terme entre deux termes successifs de même signe, le nombre des variations ne change pas ou augmente de deux variations.

Si l'on introduit un nombre quelconque de termes entre les termes d'une suite, le nombre des variations ne peut diminuer, mais il ne peut augmenter que d'un nombre pair.

Entre deux termes quelconques de signes contraires, il y a un

nombre *impair* de variations. Entre deux termes de même signe, il n'y a pas de variation ou il y a un nombre pair de variations.

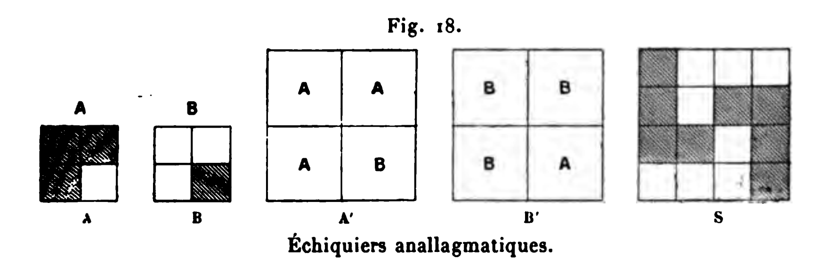
Le nombre des variations ou des permanences d'une suite ne change pas quand on change les signes de tous les termes.

Exemple I. — Échiquier anallagmatique de Sylvester. — L'échiquier anallagmatique est un carré formé de cases noires et blanches, en nombre égal ou inégal, de telle sorte que, pour deux lignes ou pour deux colonnes quelconques, le nombre de variations des couleurs est toujours égal au nombre des permanences.

On a les deux échiquiers anallagmatiques et complémentaires A et B, de deux cases de côté; aux cases blanches de l'un correspondent des cases noires dans l'autre (*fig.* 18).

Avec ces deux échiquiers, on formera de même les échiquiers complémentaires de quatre cases de côté A′ et B′. Si, dans cette figure, on remplace respectivement A et B par A′ et B′, on obtient les échiquiers complémentaires de huit cases de côté et ainsi de suite, en doublant le nombre des cases sur chaque côté. D'ailleurs, il est évident que l'on peut déduire

Fig. 18.



Échiquiers anallagmatiques.

d'un échiquier anallagmatique un grand nombre d'autres, soit en échangeant deux rangées quelconques, soit en changeant les couleurs des cases d'une rangée quelconque. Le dernier carré S est un échiquier anallagmatique indiqué par SYLVESTER; il a été reproduit comme dallage, en marbre blanc et rose.

Exemple II. — Amusements par les jetons. — Voir le n° 701 du journal *La Nature*.

CHAPITRE III.

MULTIPLICATION DES NOMBRES ENTIERS.

15. Multiplication de deux nombres entiers. — Addition abrégée de nombres égaux. *Multiplicande, multiplicateur.* — *Produit.*

Un nombre b est dit double, triple, quadruple, ..., *multiple* d'un nombre donné a, lorsqu'il est le produit de celui-ci par un nombre 2, 3, 4, ..., n.

Formation des multiples d'un nombre entier a par additions successives

$$0, \quad a, \quad 2a, \quad 3a, \quad 4a, \quad \ldots, \quad na, \quad \ldots.$$

Inversement, on dit que a est sous-double, sous-triple, ..., *sous-multiple* de b, ou qu'il en est la moitié, le tiers, le quart, ..., le $n^{\text{ième}}$. On dit encore que le nombre b est divisible par a et que celui-ci *mesure* ou *divise* b, ou encore est un *diviseur*, un *facteur* ou une *partie aliquote* de b. On doit noter la distinction entre le diviseur et la partie aliquote; ainsi b est considéré comme un diviseur de b, et n'est pas considéré comme une partie aliquote de b.

16. Multiplication des sommes algébriques. — Multiplication d'une somme algébrique par un nombre entier :

$$m(a+b-c) = ma + mb - mc.$$

Tout nombre qui en divise un autre divise tous ses multiples. Tout nombre qui en divise plusieurs autres divise la somme algébrique de multiples quelconques de ces nombres.

Multiplication de deux sommes algébriques. — Règle des signes.

17. Numération décimale. — Objet de la numération en général. — Système de numération décimale. — Numération parlée et numération écrite. — Valeurs absolues et valeurs relatives des chiffres. — Emploi du zéro.

Addition et soustraction dans le système décimal. — Méthode des compléments. — Calcul mental. — Multiplication.

Exemple I. — Exemples d'addition :

			99999
		99999	99999
	99999	99999	99999
99999	99999	99999	99999
99999	99999	99999	99999
199998	299997	399996	499995

Exemple II. — *Devinette :* On dit à une personne d'écrire trois nombres de cinq chiffres, en annonçant que l'on écrira trois autres nombres, pour former le total 299997. — Il suffit de placer au-dessous de chacun des nombres écrits par la personne des nombres dont les chiffres soient les compléments à 9 des chiffres écrits au-dessus. Le total sera 3×99999. Ce problème peut être varié de bien des manières.

Exemple III. — *La Table de Pythagore avec les deux mains.*

Si l'on sait les produits des entiers jusqu'à cinq fois cinq, on obtient le produit des autres jusqu'à neuf fois neuf par l'artifice suivant. Soit à multiplier $(5+a)$ par $(5+b)$; dans l'une des mains, on lève a doigts et l'on baisse les autres en nombre $(5-a)$; dans l'autre main, on lève b doigts et l'on baisse les autres en nombre $(5-b)$. Cela fait, le produit se compose d'un nombre de dizaines égal au nombre de tous les doigts levés, plus le produit des unités que représentent les doigts baissés. Cet artifice se vérifie par l'identité

$$(5+a)(5+b) = 10(a+b) + (5-a)(5-b).$$

Ce procédé est employé couramment en Syrie.

18. Tables de multiplication. — La première colonne et la première ligne de la Table forment la série des nombres entiers. On forme la seconde colonne en ajoutant successivement le nombre 2, la troisième colonne en ajoutant successivement le nombre 3, et ainsi de suite.

De cette façon la Table de Pythagore peut être étendue rapidement dans le sens horizontal ou dans le sens vertical. Comme vérification, les lignes et les colonnes se reproduisent de dix en dix, à partir de la première, par l'adjonction du zéro.

L'observation de la Table de Pythagore montre que *le produit de deux nombres ne change pas lorsqu'on les remplace l'un par l'autre*. On démontre ce théorème par figuration géométrique ou en faisant voir que, si l'on a

$$ab = ba,$$

on a encore des produits égaux en augmentant l'un des facteurs d'une unité, c'est-à-dire que

$$a(b+1) = (b+1)a.$$

Facteurs d'un produit. — *Preuve* de la multiplication de deux nombres inégaux.

Il existe des Tables de multiplication très étendues. Les *Rechentafeln,* par Crelle, contiennent tous les produits des nombres de trois chiffres. Pour la multiplication des nombres ayant plus de trois chiffres, on procède par *paquets* ou par tranches de trois chiffres.

Quatre éditions stéréotypées de ces *Tables de calcul*, ouvrage très pratique, ont été publiées par le Dr Bremiker (Paris, Gauthier-Villars, 1880).

Le premier ouvrage de ce genre est intitulé : *Tabulæ arithmeticæ universales,* par Hervart de Hohemburg ; il contient, en mille pages in-folio, les produits des mille premiers nombres. Il date de 1610, quatre ans avant l'apparition du *Canon mirificus,* de Neper. Pendant longtemps, l'invention des logarithmes a nui aux calculs exacts et, par suite, à la théorie des nombres.

Exemple I. — Multiplication d'un nombre par 11, 111, 1111, ... — Au lieu d'écrire le multiplicande, le multiplicateur 11, puis deux fois le multiplicande avant d'avoir le produit, on obtient tout de suite celui-ci de la manière suivante. On écrit le chiffre des unités, on ajoute le chiffre des unités à celui des dizaines, puis le chiffre des dizaines à celui des centaines, et ainsi de suite en tenant compte des retenues. Par exemple, les quatre

premières puissances de 11 sont dans le Tableau ci-dessous; ce sont les quatre premières lignes du triangle de PASCAL :

Fig. 19.

Onze....................	1 1
Carré de onze............	1 2 1
Cube de onze.............	1 3 3 1
Bicarré de onze...........	1 4 6 4 1

Puissances de onze.

De même, pour multiplier un nombre quelconque par 111, on suppose deux zéros écrits à la droite et deux zéros à la gauche du nombre donné; puis on fait successivement les sommes de trois chiffres en commençant par la droite et en tenant compte des retenues.

De même, pour multiplier par 1111, 11111, ...; on a ainsi des exemples extraits du *Talkhys* d'IBN ALBANNA (au Maroc, XIII[e] siècle).

Fig. 20.

Carré de	1	1
	1 1	1 2 1
	1 1 1	1 2 3 2 1
	1 1 1 1	1 2 3 4 3 2 1
	1 1 1 1 1	1 2 3 4 5 4 3 2 1
	1 1 1 1 1 1	1 2 3 4 5 6 5 4 3 2 1
	. . . .	. . . .

Tirée du Talkhys.

Exemple II. — Multiplication d'un nombre par 9, 99, 999, ... — Pour multiplier un nombre par 9 ou (10 — 1), on ajoute par la pensée un zéro à sa droite et l'on retranche le chiffre des unités de dix, puis celui des dizaines de celui des unités, le chiffre des centaines de celui des dizaines, et ainsi de suite, en tenant compte des retenues. Ainsi

$$12\,345\,679 \times 9 = 111\,111\,111.$$

De même, pour multiplier un nombre par 99 ou (100 — 1), on ajoute par la pensée deux zéros à sa droite, et l'on retranche successivement chacun des chiffres du deuxième à droite. Et ainsi pour 999, ...

Pour multiplier par 8, on multiplie par (10 — 2) ou par (9 — 1); voici quelques exemples curieux de multiplication :

Fig. 21.

$$12\,345\,679 \times 8 = 98\,765\,432$$

$$\begin{aligned}
1 . 9 + 2 &= 11\\
12 . 9 + 3 &= 111\\
123 . 9 + 4 &= 1111\\
1234 . 9 + 5 &= 11111\\
12345 . 9 + 6 &= 111111\\
123456 . 9 + 7 &= 1111111\\
1234567 . 9 + 8 &= 11111111\\
12345678 . 9 + 9 &= 111111111
\end{aligned}$$

$$\begin{aligned}
9 . 9 + 7 &= 88\\
98 . 9 + 6 &= 888\\
987 . 9 + 5 &= 8888\\
9876 . 9 + 4 &= 88888\\
98765 . 9 + 3 &= 888888\\
987654 . 9 + 2 &= 8888888\\
9876543 . 9 + 1 &= 88888888\\
98765432 . 9 + 0 &= 888888888
\end{aligned}$$

$$\begin{aligned}
1 . 8 + 1 &= 9\\
12 . 8 + 2 &= 98\\
123 . 8 + 3 &= 987\\
1234 . 8 + 4 &= 9876\\
12345 . 8 + 5 &= 98765\\
123456 . 8 + 6 &= 987654\\
1234567 . 8 + 7 &= 9876543\\
12345678 . 8 + 8 &= 98765432\\
123456789 . 8 + 9 &= 987654321
\end{aligned}$$

Multiplications curieuses.

Exemple III. — Carrés et produits de nombres formés d'un même chiffre. — Ces exemples sont extraits du *Talkhys*.

Fig. 22.

$9^2 =$	81	$9 \cdot 7$	$=$	63
$99^2 =$	9801	$99 \cdot 77$	$=$	7623
$999^2 =$	998001	$999 \cdot 777$	$=$	776223
$9999^2 =$	99980001	$9999 \cdot 7777$	$=$	77762223
$99999^2 =$	9999800001	$99999 \cdot 77777$	$=$	7777622223

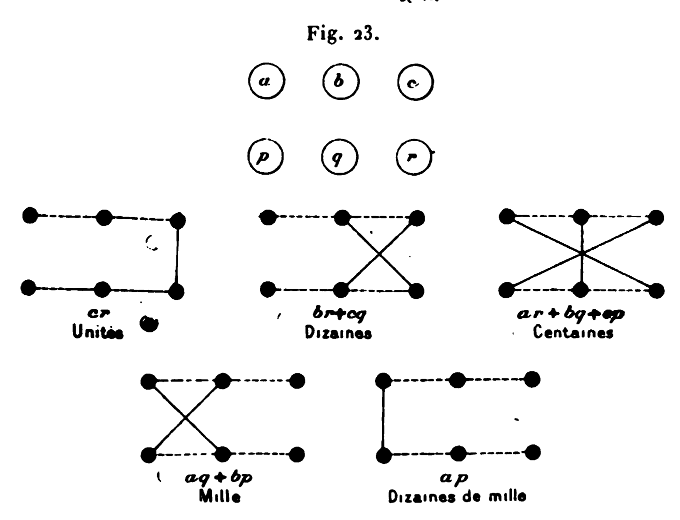
Tirée du Talkhys.

Exemple IV. — Le carré du nombre 909090909091 est un nombre formé de deux parties identiques. Il en est de même du carré de ses neuf premiers multiples.

19. Multiplication rapide. — On peut effectuer très rapidement la multiplication de nombres de deux, trois, quatre, cinq chiffres par une méthode qui se trouve exposée dans le *Liber Abbaci*. Cette méthode permet d'écrire presque immédiatement le produit, sans écrire les produits partiels. Nous l'expliquerons sur deux nombres de trois chiffres; si les facteurs n'ont pas le même nombre de chiffres, on complète l'un d'eux par des zéros ajoutés soit à droite, soit à gauche.

Soient (*fig.* 23) abc et pqr deux nombres écrits dans le système décimal. On forme le produit cr; on écrit le chiffre des unités de ce produit, et l'on ajoute la retenue aux deux produits br et cq

Fig. 23.



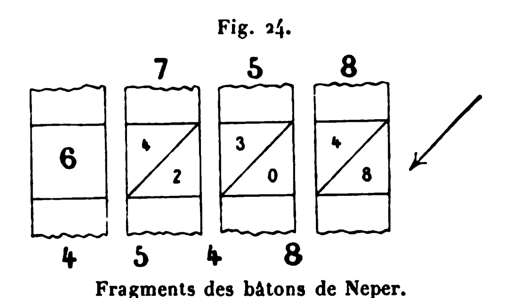
Multiplication rapide, au XIIIe siècle.

qui représentent les dizaines; on écrit le chiffre des unités de ce total qui est le chiffre des dizaines du produit, et l'on ajoute la retenue à la somme des centaines $ar + bq + cp$, et ainsi de suite, conformément au Tableau (*fig.* 23).

20. Bâtons népériens. — JEAN NEPER, baron de Markinston, en Écosse, a indiqué en 1617, dans sa *Rhabdologie,* une ingénieuse

méthode de calcul pour simplifier la multiplication et la division. Le tableau chiffré (*fig.* 24) représente la Table de Pythagore découpée en dix bâtons ou planchettes : la planchette à gauche est fixe; toutes les autres sont mobiles et peuvent être permutées de toutes les façons. Pour l'enseignement, on les appuie sur un tableau muni d'une rangée de clous sur la ligne horizontale supérieure; on peut y suspendre les planchettes, préalablement percées d'une ouverture à la partie supérieure. Chacun des carrés de la Table est divisé en deux triangles, par une diagonale; dans le triangle du bas, on trouve les unités de chacun des produits, dans celui du haut et à gauche se trouve le chiffre des dizaines. Supposons que l'on ait placé à côté de la barre fixe, à gauche, les tablettes portant en haut et en bas les nos 7, 5, 8, on obtient presque immédiatement les produits de 758 par tous les nombres, de 1 à 9. Ainsi, par exemple, devant le 6 de la colonne fixe, on trouve horizontalement et en

Fig. 24.



Fragments des bâtons de Neper.

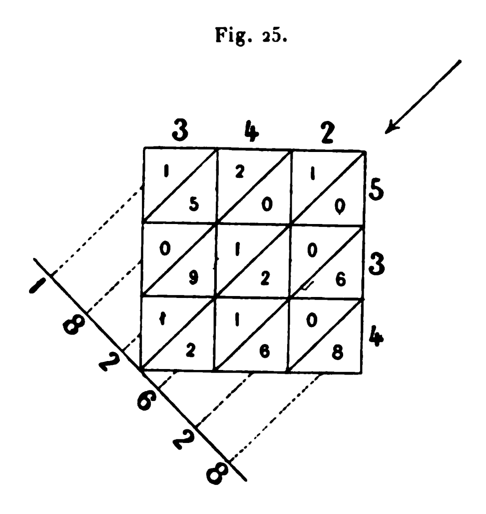
faisant l'addition parallèlement à la diagonale ↙ des carrés, le produit 4548, qui est le produit de 758 par 6. De même, pour les autres produits par 2, 3, 4, 5, 6, 7, 8, 9.

Donc les *réglettes* de Neper permettent de trouver rapidement, sans qu'il soit nécessaire de savoir sa Table de Pythagore, mais par une simple addition de deux chiffres, tous les produits partiels d'un nombre de dix chiffres et plus. Ainsi, la multiplication se trouve ramenée à l'addition, et cette opération se trouve d'autant plus facilitée qu'il s'agit de nombres de plus en plus grands.

La belle invention de Neper provient peut-être d'une remarque sur l'une des nombreuses manières d'effectuer la multiplication chez les Persans et chez les Arabes. Voici, par exemple, la copie de la multiplication de 534 par 342 tirée du *Traité d'Arithmétique* d'Aboul Haçan Ali ben Moham-

MED, le *Koraïchite,* plus connu sous le nom d'Alkalçadi, auteur arabe qui mourut vers 1480. Nous avons tenu compte de la différence d'orientation de l'écriture arabe avec la nôtre (*fig.* 25).

Fig. 25.



Multiplication arabe par réseaux.

21. Réglettes multiplicatrices. — Dans un Mémoire sur les moyens de faciliter le calcul, publié dans les *Annales de Mathématiques* (t. VII, 1817), Gergonne approuve l'emploi des baguettes de Neper et constate qu'après la découverte des logarithmes elles tombèrent dans un oubli absolument immérité.

D'autres essais du même genre n'ont pas été plus heureux, parce que ces baguettes ne donnent que les produits partiels de la multiplication, c'est-à-dire les multiplications de nombres quelconques par les neuf premiers nombres. Il a été aussi publié des Tables de tous les produits des nombres de quatre et cinq chiffres, par des nombres d'un seul chiffre; en particulier, on doit citer celles de Cadet publiées à Paris, en 1797; celles de Bretschneider, à Gotha, en 1827; et, plus récemment, les Tables de Tripier. Cependant l'emploi de ces Tables, pour les grands calculs, est inférieur à l'usage des *réglettes népériennes,* surtout lorsque l'on se sert de réglettes imprimées sur les quatre faces, ou de rouleaux népériens.

Le Conservatoire des Arts et Métiers possède une importante

collection d'appareils de ce genre, parmi lesquels nous citerons plus particulièrement l'appareil de M. DE MAXIMOVITCH, qui permet d'imprimer instantanément les colonnes de la Table de Pythagore dans un ordre quelconque. Nous citerons aussi les réglettes de M. PRUVOST-LE-GUAY publiées à Paris, en 1890, avec des améliorations successives, dans lesquelles les bâtons de Neper sont réunis par deux, ce qui simplifie considérablement leur emploi.

On a aussi cherché à supprimer l'addition de deux chiffres dans l'emploi des bâtons de Néper. Nous devons rappeler les essais intéressants du Dr ROTH, dans son *Prompt multiplicateur et diviseur,* publié à Paris, en 1841. Mais nous devons signaler surtout les réglettes de GENAILLE qui donnent sans aucune addition tous les produits partiels.

Nous avons publié à la librairie BELIN, à Paris, en 1885, en collaboration avec M. GENAILLE, quatre boîtes de réglettes pour la simplification des calculs, à savoir :

I. Les *Réglettes multiplicatrices,* appareils à calculs exacts et instantanés pour simplifier la multiplication et la division.

II. Les *Réglettes multisectrices,* appareils à calculs exacts et instantanés pour simplifier la division.

III. Les *Réglettes financières* pour simplifier les calculs financiers et commerciaux.

IV. Les *Réglettes népériennes*, joujoux calculateurs ayant pour but de simplifier l'étude et de faciliter la pratique des opérations de l'Arithmétique.

Depuis quelques années, M. GENAILLE a su résoudre, d'une manière simple et complète, le problème difficile de la multiplication et de la division des grands nombres par une méthode absolument géométrique; mais ses admirables appareils sont encore inédits.

22. Du produit de plusieurs facteurs. — La notation

$$a \times b \times c \times d \quad \text{ou} \quad a.b.c.d \quad \text{ou} \quad abcd$$

indique le résultat de l'opération obtenue en multipliant d'abord a par b, puis le produit par c, puis le nouveau produit par d.

Si deux produits contiennent les mêmes facteurs en nombre n, mais dans deux ordres différents, et si l'on augmente l'un des facteurs d'une unité, on voit que ces produits augmentent tous deux

du produit des $(n-1)$ autres facteurs pris dans leurs ordres respectifs. Par suite, on aura ainsi pour cinq facteurs

$$1.1.1.1.1 = 1.1.1.1.1,$$
$$1.1.a.1.1 = 1.1.1.1.a,$$
$$b.1.a.1.1 = 1.1.b.1.a,$$
$$b.1.a.1.c = c.1.b.1.a,$$
$$b.d.a.1.c = c.1.b.d.a,$$
$$b.d.a.e.c = c.e.b.d.a.$$

Le résultat du produit successif d'un nombre quelconque d'entiers positifs est indépendant de l'ordre dans lequel on effectue les multiplications. En outre, puisque l'ordre des facteurs est indifférent, on peut toujours supposer que deux d'entre eux occupent les deux premiers rangs, et les remplacer par leur produit, ou inversement.

Par conséquent, si l'on considère le produit d'un nombre quelconque d'entiers positifs, on peut remplacer deux d'entre eux par leur produit et opérer sur le nouvel ensemble de facteurs comme sur le premier, et ainsi jusqu'à ce que l'on arrive à un seul produit, qui sera toujours indépendant de l'ordre et du choix des multiplications opérées sur deux facteurs (*voir* n° 43, *Exemple V*).

Multiplier un nombre par le produit effectué de plusieurs facteurs revient à multiplier ce nombre successivement par chacun des facteurs du produit.

Pour multiplier un produit par un certain nombre, il suffit de multiplier par ce nombre un des facteurs du produit.

23. Puissances d'un nombre. — *Carrés, cubes, bicarrés.* — Degré d'une puissance. — Notation des exposants.

Règles des exposants. — On a les deux formules

$$a^p.a^q.a^r = a^{p+q+r},$$
$$[(a^p)^q]^r = a^{pqr}.$$

Il ne faut pas confondre la notation $(a^p)^q$ avec la notation

a^{p^q} qui veut dire $a^{(p^q)}$.

Multiplication des monômes. — On multiplie les coefficients et l'on ajoute les exposants.

Exemple I. — Les derniers chiffres des puissances (*résidus potentiels* dans le système décimal) sont

1res puissances	0	1	2	3	4	5	6	7	8	9
2es »	0	1	4	9	6	5	6	9	4	1
3es »	0	1	8	7	4	5	6	3	2	9
4es »	0	1	6	1	6	5	6	1	6	1
5es »	0	1	2	3	4	5	6	7	8	9
6es »	0	1	4	9	6	5	6	9	4	1
7es »	0	1	8	7	4	5	6	3	2	9
8es »	0	1	6	1	6	5	6	1	6	1

Les cinquièmes puissances sont terminées comme les premières; cette remarque a donné naissance au théorème de FERMAT. Les derniers chiffres des puissances successives d'un nombre se reproduisent périodiquement de quatre en quatre.

Tout bicarré est terminé par l'un des chiffres 0, 1, 5, 6.

Exemple II. — Former les puissances successives de 2. — En doublant continuellement, on forme la suite des nombres

$$1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ 256,\ 512,\ 1024,\ \ldots;$$

on vérifie les calculs par les résultats suivants :

$$2^{16} = 65536,$$
$$2^{32} = 42949\ 67296,$$
$$2^{64} = 18446\ 74407\ 37095\ 51616;$$

la puissance de 2 d'exposant 196, égale à seize fois le cube de la précédente, se compose des soixante chiffres suivants :

10043 36277 66186 89222 13726 30771
32266 26576 37687 11142 45522 06336.

Exemple III. — Vérifier la formule

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1.$$

Exemple IV. — Former les puissances successives de 5. On en trouve une table étendue dans la Préface des *Tables de logarithmes* de CALLET.

Exemple V. — Le chiffre des dizaines de mille d'une puissance quelconque de 5, ne peut être ni un 3, ni un 8. (LAISANT.)

24. Table des carrés. — Si l'on remplace la première colonne des 1 du triangle arithmétique par des 2, on forme un autre Tableau de sommes. Alors la seconde colonne représente les nombres *im-*

pairs; la troisième colonne représente les nombres *carrés,* comme cela résulte immédiatement de la formule

$$\Delta n^2 = (n+1)^2 - n^2 = 2n+1.$$

En d'autres termes, les accroissements successifs des carrés sont les nombres impairs, et la somme des n premiers impairs

$$1,\ 3,\ 5,\ \ldots,\ 2n-1,$$

est égale au carré n^2 de leur nombre. Ces procédés étaient connus de Pythagore et de Platon.

Fig. 26.

	0	1	2	3	4	5	6
0	2	1					
1	2	3	1				
2	2	5	4	1			
3	2	7	9	5	1		
4	2	9	16	14	6	1	
5	2	11	25	30	20	7	1

Table des carrés.

On peut ainsi construire rapidement une Table des carrés, par additions successives, en se bornant aux trois premières colonnes du Tableau. On vérifie les calculs de dix en dix lignes, par les carrés déjà formés, en ajoutant deux zéros. L'économie de ce calcul est considérable, puisque, pour calculer la table des mille premiers carrés, il suffit de mille additions, au lieu de mille multiplications; d'autre part, cette méthode de calcul par différences possède l'immense avantage de présenter continuellement la vérification des calculs, de dix en dix lignes, ainsi que nous venons de le dire, tandis que la méthode directe des multiplications est incertaine pour chaque multiplication; on ne peut faire la preuve du résultat par l'interversion des deux facteurs du produit, puisque ceux-ci sont égaux.

Les propriétés du triangle arithmétique subsistent dans ce Tableau; mais on voit que chacun de ses termes peut se déduire du triangle de Pascal, en ajoutant aux termes de ceux-ci les termes obtenus en baissant d'une ligne le triangle arithmétique. Si l'on

ou les *résidus quadratiques,* dans le système décimal, et que les nombres 2, 3, 7, 8 ne le sont pas.

Cette remarque si simple a donné naissance, en supposant les nombres écrits dans un système quelconque de numération, à la théorie des résidus quadratiques, qui sera développée ultérieurement.

Exemple I. — Le chiffre des dizaines d'un carré terminé par 1 ou par 9 est un nombre pair.

Le chiffre des dizaines d'un carré terminé par 5 est 2.

Le chiffre des dizaines d'un carré terminé par 4 est un nombre pair.

Le chiffre des dizaines d'un carré terminé par 6 est un nombre impair; réciproquement, si le chiffre des dizaines d'un carré est impair, le chiffre des unités est 6.

Un nombre n'est pas un carré parfait, si l'ensemble de ses deux derniers chiffres n'est pas l'un des vingt-deux nombres

00; 01, 21, 41, 61, 81; 04, 24, 44, 64, 84;
25; 09, 29, 49, 69, 89; 16, 36, 56, 76, 96.

Dans ses *Nouveaux Éléments de Mathématiques* (1689), **Prestet** donne la table des quatre derniers chiffres des carrés.

Exemple II.— Toute somme de deux carrés a un nombre pair de dizaines, si elle est terminée par 1, 5, 9, et un nombre impair de dizaines, si elle est terminée par 3 ou par 7.

Exemple III. — Le carré d'un nombre terminé par 8 212 890 625 se termine de la même façon, et il n'y a qu'un seul autre nombre de dix chiffres (en exceptant dix zéros, ou neuf zéros suivis de 1), qui possède la même propriété; c'est le nombre 1 787 109 376.

Exemple IV. — Trouver les n derniers chiffres d'un nombre, connaissant les n derniers chiffres de son carré. — Par exemple, si les neuf derniers chiffres du carré d'un nombre sont 224 406 889, les neuf derniers chiffres de ce nombre sont parmi les groupes suivants :

265 810 083; 765 810 083; 363 466 333; 863 466 333;
734 189 917; 234 189 917; 636 533 667; 136 533 667.

Exemple V. — Connaissant le produit d'un nombre par le nombre renversé, retrouver les facteurs du produit.

Voir une Note de M. Laisant dans les *Mémoires de la Société des Sciences physiques et naturelles* (Bordeaux, 1876).

CHAPITRE IV.

DIVISION ET CLASSIFICATION DES ENTIERS.

27. Division des entiers. — La division est une soustraction abrégée de nombres égaux à un nombre donné. Définitions du *dividende,* du *diviseur,* du *quotient* et du *reste* de la division.

Le dividende est égal au produit du diviseur par le quotient, augmenté du reste.

Opération de la division dans le système décimal. Nombre des chiffres du quotient.

Preuve de la division par la multiplication.

Dans le cas de la division exacte de a par b, on désigne le quotient par l'une ou l'autre des notations

$$a : b \quad \text{ou} \quad \frac{a}{b};$$

dans le cas de la division exacte, ou approchée à une unité près *par défaut,* on désigne le quotient de a par b, au moyen du symbole

$$\mathrm{E}\frac{a}{b} \quad \text{ou} \quad \left[\frac{a}{b}\right].$$

Division approchée *par excès* à une unité près.

Division la plus approchée. — *Reste minimum.*

On a les propriétés suivantes :

I. Lorsque l'on multiplie le dividende et le diviseur d'une division par un même nombre, le quotient ne change pas, mais le reste est multiplié par ce nombre.

II. Diviser un nombre par un produit effectué de plusieurs facteurs revient à diviser ce nombre successivement par chacun des facteurs du produit, et réciproquement.

III. Lorsque les divisions donnent lieu à des restes, le principe précédent subsiste pour la partie entière du quotient.

Exemple I. — Le nombre 9 est, de diverses manières, égal au quotient de deux nombres de cinq chiffres, en supposant tous les chiffres distincts. En effet, 9 est le quotient des divisions

$$\frac{97524}{10836}, \quad \frac{95823}{10647}, \quad \frac{95742}{10638}, \quad \frac{75249}{08361}, \quad \frac{58239}{06471}, \quad \frac{57429}{06381}.$$

Exemple II. — Le nombre 100 peut être écrit sous forme d'entier augmenté du quotient d'une division, avec les neuf chiffres significatifs pris une seule fois, des diverses manières suivantes :

$$91\ \frac{5742}{638}, \quad 91\ \frac{7524}{836}, \quad 91\ \frac{5823}{647}, \quad 94\ \frac{1578}{263},$$

$$96\ \frac{2148}{537}, \quad 96\ \frac{1428}{357}, \quad 96\ \frac{1752}{438}.$$

Exemple III. — On écrit tous les nombres du système décimal à la suite les uns des autres; quel est le chiffre de rang donné? Si l'on partage les nombres en groupes de 1, 2, 3, 4, ... chiffres, le nombre des chiffres du

1er groupe est.....	9×1	ou	1×9,
2e » ».....	90×2	»	20×9,
3e » ».....	900×3	»	300×9,
4e » ».....	9000×4	»	4000×9,
5e » ».....	90000×5	»	50000×9.

Ainsi le total des chiffres des nombres des cinq premiers groupes est égal à 54321×9; celui des six premiers groupes est 654321×9, etc. Si l'on veut savoir quel est le 75892e chiffre de la suite, on remarque que ce chiffre appartient à un nombre de cinq chiffres; mais le nombre des chiffres des quatre premiers groupes est 38889. De plus,

$$75892 - 38889 = 37003,$$

et

$$37003 = 7400 \times 5 + 3;$$

ainsi le chiffre cherché est le troisième du 7401e nombre de cinq chiffres, c'est-à-dire $10000 + 7400$. Donc le chiffre demandé est 4.

Exemple IV. — On peut se proposer des questions analogues à la précédente, en n'écrivant : 1° que les nombres pairs; 2° que les nombres impairs; 3° que les chiffres pairs; 4° que les chiffres impairs.

28. Division accélérée. — Lorsque le diviseur contient beaucoup de chiffres, on simplifie le calcul de la manière suivante. On écrit sur une bande de papier les dix premiers multiples du diviseur, que l'on forme par additions successives, avec preuve au

moyen du dixième multiple. Puis l'opération se réduit à une suite de soustractions; elle s'accélère en pliant la bande de papier sous chacun des multiples; on la tient de la main gauche au-dessus des dividendes partiels, que l'on écrit successivement par une simple soustraction. Cette méthode, très pratique, supprime les essais pour déterminer chaque chiffre du quotient; elle est surtout avantageuse lorsqu'il s'agit de diviser plusieurs nombres par un même diviseur.

Si l'on ne veut pas calculer les dix premiers multiples, on peut employer les Tables de Tripier, les réglettes de Neper ou de Pruvost-le-Guay, ou encore les réglettes de Genaille.

Exemple I. — Division d'un nombre par 9. — Soit le nombre 23547 à diviser par 9. On fait la somme des chiffres en partant de la droite, soit 21, dont le quotient par 9 est 2, que l'on ajoute à la somme des chiffres à partir des dizaines, et en comptant de droite à gauche, soit 16; on pose 6 et l'on retient 1 que l'on ajoute à la somme des chiffres de droite à gauche, en partant des centaines, soit 11; on pose 1, chiffre des dizaines et l'on retient 1 que l'on ajoute à la somme des chiffres en partant des mille; soit 6, que l'on pose, et enfin 2, à partir des dizaines de mille. Le quotient est 2616.

En général, soit $(abcde)$ un nombre écrit dans le système décimal, et que l'on veut diviser par 9; on a

$$\begin{aligned} a.10^4 &= 9999.a + a, \\ b.10^3 &= 999.b + b, \\ c.10^2 &= 99.c + c, \\ d.10 &= 9.d + d, \\ e. &= e; \end{aligned}$$

et, en ajoutant et en divisant par 9,

$$\begin{aligned} \mathrm{E}\frac{abcde}{9} = \mathrm{E}&\frac{e+d+c+b+a}{9} \\ &+ d + c + b + a \\ &+ 10\,(c + b + a) \\ &+ 10^2(b + a) \\ &+ 10^3.a. \end{aligned}$$

29. Systèmes de numération. — Pour classer les nombres, pour étudier leurs propriétés, leurs combinaisons et leurs transformations, on peut employer divers systèmes de numération, et plus particulièrement celui de la numération décimale.

C'est aux Chinois et aux Hindous que l'on doit l'idée ingénieuse de ces échelles arithmétiques, de cet heureux moyen de représenter tous les nombres avec peu de signes, et d'exécuter, par des opérations techniques très simples, des calculs auxquels l'intelligence humaine, livrée à elle-même, ne pourrait atteindre. « C'est là, dit Condorcet, le premier exemple de ces méthodes qui doublent ses forces, et à l'aide desquelles elle peut reculer indéfiniment ses limites, sans qu'on puisse fixer un terme où il lui soit interdit de parvenir. »

Tout nombre entier, autre que l'unité, peut être pris pour base d'un système de numération. On a ainsi les systèmes de numération *binaire, ternaire, quaternaire, ..., décimale, duodécimale,* qui correspondent aux bases deux, trois, quatre, ..., dix, douze.

Pour écrire un nombre dans un système de base B, on commence par adopter (B — 1) caractères destinés à représenter les (B — 1) premiers nombres. Ces caractères sont les *chiffres*

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ a,\ b,\ c,\ \ldots,$$

que l'on énonce comme à l'ordinaire.

Pour la *numération écrite,* on fait cette convention, qu'un chiffre, placé à la gauche d'un autre, représente des unités de l'ordre immédiatement supérieur, ou B fois plus grandes. Pour tenir la place des unités qui peuvent manquer dans certains ordres, on se sert du zéro, o; par suite, le nombre des chiffres employés est toujours égal à la base du système.

Pour la *numération parlée,* on convient d'appeler *unité* simple, *dizaine, centaine, mille,* etc., les unités du premier ordre, du second, du troisième, du quatrième, etc. Ainsi les nombres 10, 11, ..., 19 se liront de même dans tous les systèmes de numération; les nombres $1a$, $1b$, $a0$, $b0$, ... se liront *dix-a*, *dix-bé*, *a-dix*, *bé-dix*, etc. Et $5b6a71c$ se lira *cinq millions bé-cent, soixante-a mille sept cent dix-cé.*

Les règles des opérations démontrées pour les nombres écrits dans le système décimal sont les mêmes pour les nombres écrits dans un système quelconque de numération.

Pour opérer rapidement dans un système quelconque de numération, il est indispensable de savoir par cœur toutes les sommes et tous les produits de deux nombres d'un seul chiffre.

Aristote avait observé que le nombre 4 pouvait très bien remplacer le nombre 10, comme base de la numération. Weigel publia à ce sujet, en 1687, le plan d'une *Arithmétique tétractique*. Simon Stevin, de Bruges, mort en 1633, avait aussi imaginé le système de numération duodécimale, se rapprochant beaucoup plus de notre manière de compter les mois de l'année, les heures du jour, les degrés de la circonférence. Quant au système de la numération binaire, auquel nous avons consacré deux Chapitres dans nos *Récréations mathématiques,* il date de cinquante-quatre siècles; il fut retrouvé par Leibniz.

On peut donc se demander si l'adoption d'une base autre que dix n'eût pas été préférable; en d'autres termes, si l'accident de notre espèce qui fait que nous avons dix doigts aux deux mains s'accorde avec les conditions requises pour que le système de numération chiffrée soit le plus parfait possible. Ceci exige qu'on distingue la notation des nombres entiers et abstraits de celle des nombres concrets et fractionnaires. Sous le rapport de l'application du système de numération à celui des mesures, et à la subdivision de l'unité concrète, on est convenu, ainsi que Buffon l'a remarqué, que le nombre *douze,* à cause de ses quatre diviseurs : deux, trois, quatre, six, eût été une base plus commode que le nombre dix, qui n'a que deux diviseurs : deux et cinq.

D'autre part, Auguste Comte avait remarqué que la structure de la main, composée de quatre doigts à trois phalanges, ou de douze phalanges, permet de représenter avec les deux pouces posés sur deux phalanges tous les nombres jusqu'à treize fois douze; alors les phalanges de la main gauche représentent des unités simples, et celles de la main droite des *grosses,* ou unités de second ordre. Par suite, on pourrait ainsi compter sur ses phalanges dans le système duodécimal, plus facilement et plus loin que sur ses doigts dans le système décimal. Mais, si l'on se reporte au *Calcul digital,* ignoré de Comte, cette assertion est inexacte. Au moyen de ce calcul, professé dans les écoles, au temps de Charlemagne, on représentait avec les doigts des deux mains tous les nombres jusqu'à dix mille.

Il serait plutôt permis de se demander si le choix d'une base inférieure à dix ne rendrait pas les calculs plus sûrs et plus faciles. En effet, B désignant la base du sytème de numération, il faut retenir de mémoire les $\frac{1}{2}(B-1)(B-2)$ valeurs différentes de la somme et du produit de deux nombres inégaux, et les $(B-1)$ valeurs des premiers carrés, des premiers cubes. Par conséquent, les premiers frais de mémoire diminuent avec la base et les causes d'erreur seront moindres. Mais cet avantage est compensé par la nécessité d'employer plus de temps et de place pour écrire les nombres.

30. Échange des systèmes de numération. — Il s'agit d'écrire dans un autre système de base donnée un nombre quelconque écrit dans un premier système. De là, trois problèmes à résoudre.

Exemple V. — Tout nombre entier est la somme algébrique de puissances de 3, toutes différentes.

Voir, dans nos *Récréations mathématiques*, l'application du système binaire aux *Boites de Poids*, au *Baguenaudier*, à l'*Éventail japonais*, au *Jekim*, à la *Tour d'Hanoï*.

31. Classification des nombres. — Par rapport à une *base* ou *module positif* M, tout nombre entier quelconque a, positif ou négatif, peut se mettre d'une seule manière sous la *forme linéaire*

$$a = Mx + r,$$

dans laquelle r désigne l'un des M nombres positifs

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad (M-1).$$

Le nombre x est le quotient, positif ou négatif, de a par M à une unité près par défaut. D'ailleurs, si l'on avait de deux manières

$$a = Mx + r \qquad \text{et} \qquad a = Mx' + r',$$

la différence nulle

$$M(x - x') + r - r',$$

et, par suite, $(r - r')$ serait divisible par M, ce qui est impossible à moins de supposer $r = r'$. Le nombre r est appelé *reste* de a pour le module M.

Exemple. — Pour le module $M = 2$, il y a deux formes de nombres, les *pairs* et les *impairs*; pour le module $M = 3$, il y a trois formes de nombres; pour le module $M = 4$, il y en a quatre, savoir :

$4M$ pairement pairs,
$4M + 1$ pairement impairs,
$4M + 2$ impairement pairs,
$4M + 3$ impairement impairs.

En acceptant les restes négatifs, un nombre entier quelconque est encore d'une seule manière de la forme

$$a = Mx \pm r,$$

et le reste minimum r ne peut surpasser en valeur absolue la moitié du module. Dans le cas de M pair, on convient de prendre

avec le signe + le reste égal en valeur absolue à la moitié du module.

Exemple. — Pour le module $M = 5$, tous les entiers sont, d'une seule manière, de l'une des cinq formes

$$5x, \quad 5x \pm 1, \quad 5x \pm 2,$$

et pour le module $M = 6$, tous les entiers sont de l'une des six formes

$$6x, \quad 6x \pm 1, \quad 6x \pm 2, \quad 6x + 3.$$

32. Nombres congrus ou équivalents pour un module. — Deux nombres entiers a et b, positifs ou négatifs, sont dits *congrus* ou *équivalents* pour le module M lorsque leur différence est divisible par le module. Pour exprimer cette relation, on peut écrire

$$a = b + \text{mult. de } M;$$

mais il est plus commode de se servir de la notation de Gauss

$$a \equiv b \pmod{M},$$

qui se lit *a congru à b*, pour le module M. D'autre part, on a étendu la signification du mot *reste* en disant que deux nombres congrus pour le module M sont *résidus l'un de l'autre* pour ce module.

L'égalité entre deux nombres, en supprimant les multiples du module, s'appelle *congruence* ou *équivalence*. La notation de Gauss permet de mettre en évidence l'analogie qui existe entre les égalités et les congruences, sans introduire de confusion.

Pour un même module, deux nombres congrus à un troisième sont congrus entre eux.

On peut ajouter ou retrancher membre à membre des congruences de même module.

On peut multiplier les deux membres d'une congruence par un même nombre entier.

On peut multiplier membre à membre les congruences de même module.

On peut élever à une même puissance les deux membres d'une congruence.

En d'autres termes, si l'on a, pour le module M, les congruences

$$a \equiv b, \qquad a' \equiv b', \qquad a'' \equiv b'',$$

on a encore

$$a - a' + a'' \equiv b - b' + b'',$$
$$\lambda a + \mu a' + \nu a'' \equiv \lambda b + \mu b' + \nu b'',$$
$$aa'a'' \equiv bb'b'',$$
$$a^m \equiv b^m.$$

Plus généralement, si l'on désigne par $f(x)$ un polynôme à coefficients entiers, positifs ou négatifs,

$$f(x) = Ax^n + Bx^{n-1} + Cx^{n-2} + \ldots + Kx + L,$$

la congruence

$$a \equiv b \pmod{M},$$

donne aussi

$$f(a) \equiv f(b) \pmod{M}.$$

33. **Impossibilité de congruences.** — Si l'on remplace successivement x par tous les nombres entiers dans un polynôme $f(x)$ à coefficients entiers, et si l'on prend les résidus pour le module M, ces restes se reproduisent périodiquement de M en M, puisque l'on a, quel que soit l'entier x,

$$f(x) \equiv f(x + M) \pmod{M}.$$

Ainsi, par exemple, pour $f(x) = x^2$ et pour $M = 10$, on retrouve les restes des carrés. En général, la suite des résidus de $f(x)$ pour M valeurs entières et consécutives de x ne reproduit pas la série des M nombres

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad (M - 1);$$

on en déduit alors l'impossibilité de résoudre la congruence

$$f(x) \equiv r \pmod{M},$$

en nombres entiers, si r désigne l'un quelconque des *non-résidus*.

Par exemple, pour $M = 5$, les restes de

$$f(x) = x^3 - 8x + 6$$

forment la suite périodique

$$1,\ 4,\ 3,\ 4,\ 3;$$

par suite, $f(x)$ ne peut devenir $\equiv 0$, ni $\equiv 2$, pour le module 5 et, *a fortiori*, égal à 2 ou à 5 ; d'où il suit que les expressions

$$x^3 - 8x + 6 \quad \text{et} \quad x^3 - 8x + 4,$$

ne peuvent s'annuler pour des valeurs entières de x, ni lorsque l'on augmente les coefficients d'un multiple quelconque de 5.

Exemple I. — Le polynôme $f(x)$ à coefficients entiers ne peut s'annuler pour une valeur entière de x, si $f(0)$ et $f(1)$ sont impairs.

De même, si aucun des nombres $f(0)$, $f(1)$ et $f(-1)$ n'est divisible par 3.

34. Preuves par congruences. — La preuve par 9 dans le système de numération décimale, pour les quatre opérations fondamentales de l'Arithmétique, repose sur les théorèmes que nous venons d'énoncer sur les congruences, en supposant $M = 9$. En effet, suivant le module $M = 9$, toutes les puissances de dix sont congrues à l'unité, puisque $10^n - 1$, étant un nombre formé exclusivement des chiffres 9999...., est divisible par 9. Par conséquent, si $a, b, c, d, \ldots$ désignent respectivement les chiffres des unités, dizaines, centaines, ... d'un nombre N écrit dans le système décimal, on a

$$N = a + 10b + 10^2c + 10^3d + \ldots,$$

et, par suite

$$N \equiv a + b + c + d + \ldots \pmod 9.$$

En d'autres termes, le reste de la division d'un nombre par 9 est égal au reste de la division par 9, de la somme de ses chiffres.

De même, pour le module $M = 11$, on a successivement

$$10 \equiv -1, \qquad 10^2 \equiv +1, \qquad 10^3 \equiv -1, \qquad \ldots;$$

et, par suite,

$$N \equiv a - b + c - d + \ldots \pmod{11}.$$

Par conséquent, si l'on remplace, dans les quatre opérations fondamentales de l'Arithmétique, les nombres donnés par leurs restes suivant le module 9 ou le module 11, les nombres obtenus doivent

être congrus à ceux qu'on déduirait des résultats; sinon il y aurait erreur dans les calculs.

Plus généralement, si θ désigne la base d'un système de numération, on a vu que tout nombre positif N peut être mis, d'une seule manière, sous la forme

$$N = a + b\theta + c\theta^2 + d\theta^3 + \ldots,$$

les nombres $a, b, c, d, \ldots$ étant positifs ou nuls et plus petits que θ. D'ailleurs, si l'on désigne par x le quotient approché par défaut de N par θ, à une unité près, le chiffre a des unités est le reste minimum, non négatif, de N suivant le module θ, et l'on a

$$x = b + c\theta + d\theta^2 + \ldots,$$

et ainsi de suite. D'ailleurs $(\theta^n - 1)$, nombre formé exclusivement par les chiffres $(\theta - 1)$, est un multiple de $(\theta - 1)$; on a donc

$$N \equiv a + b + c + d + \ldots \pmod{\overline{\theta - 1}}.$$

De même, pour le module $(\theta + 1)$, on a

$$\theta \equiv -1 \pmod{\overline{\theta + 1}};$$

en élevant à la puissance d'exposant n,

$$\theta^n \equiv (-1)^n \pmod{\overline{\theta + 1}};$$

et, par suite,

$$N \equiv a - b + c - d + \ldots \pmod{\overline{\theta + 1}}.$$

Par conséquent, dans un système de base quelconque θ, on peut faire les preuves des opérations par congruences suivant les modules $(\theta - 1)$ et $(\theta + 1)$.

Ces considérations s'appliquent encore aux systèmes de numération dans lesquels on considère des chiffres à caractéristique négative. Ainsi tout nombre positif N peut être mis sous la forme

$$N = a + b\theta + c\theta^2 + d\theta^3 + \ldots + l\theta^n;$$

les nombres $a, b, c, d, \ldots$ sont des entiers nuls, positifs ou négatifs, dont la valeur absolue ne surpasse pas la moitié de θ, l seul étant nécessairement positif. La représentation de N est encore unique, à la condition de supposer pour θ pair que le nombre égal à $\pm \frac{1}{2}\theta$ soit toujours pris avec le signe $+$.

Si l'on groupe les chiffres d'un nombre quelconque par *tranches* de deux, trois, quatre, ..., n chiffres, à partir des unités du premier ordre, on peut considérer ces tranches comme des chiffres et supposer le nombre N écrit dans un système de numération qui aurait pour base l'un des nombres $\theta^2, \theta^3, \theta^4, \ldots, \theta^n$. De là des règles de divisibilité et des preuves par congruences pour les modules $(\theta^n - 1)$ et $(\theta^n + 1)$.

Ainsi, par exemple, $10^3 + 1 = 7.11.13$; par conséquent, on en déduit des règles de divisibilité et des preuves par 7, 11 ou 13, en considérant les nombres écrits dans le système décimal, par tranches de trois chiffres.

Exemple I. — Démontrer que $2^{32} + 1$ est divisible par 641 (EULER).

On a, pour le module 641,

$$2^2 = 4, \quad 2^4 = 16, \quad 2^8 = 256,$$
$$2^{16} = 65536 \equiv 154,$$
$$2^{32} \equiv 23716 \equiv -1.$$

On démontre de même que

$2^{2^6} + 1$	est divisible par	.....	274 177,
$2^{2^{12}} + 1$	»	.....	114 689,
$2^{2^{23}} + 1$	»	.....	167 772 161,
$2^{2^{36}} + 1$	»	.....	2 748 779 069 441.

Ce dernier exemple prouve que le calcul par congruences est parfois indispensable, attendu qu'il est impossible d'écrire le nombre $2^{2^{36}} + 1$, qui a plus de 20 milliards de chiffres; la bande de papier qui le contiendrait ferait le tour de la Terre. D'ailleurs, on ne connaît pas d'autre démonstration de ce curieux résultat, dû à M. SEELHOFF, de Brême.

Exemple II. — Le produit de nombres de la forme linéaire $Mx + 1$ est un nombre de la même forme.

Le produit de nombres de la forme $4x + 3$ est de la forme $4x + 1$ si le nombre des facteurs est pair, et de la forme $4x + 3$ si le nombre des facteurs est impair.

De même, pour les nombres de la forme $Mx - 1$.

Exemple III. — Le cube d'un nombre entier est congru à 0 ou à ± 1, suivant le module 9.

Si un nombre n'est pas un cube parfait, tout nombre formé en permutant les chiffres du premier d'une manière quelconque, et en intercalant des 0 et des 9, n'est pas un cube parfait.

CHAPITRE V.

LES NOMBRES FIGURÉS.

35. **Progressions arithmétiques.** — *Définitions et propriétés.* — Nous désignerons les termes de la progression par

$$\div a,\ b,\ c,\ \ldots,\ h,\ k,\ l,$$

la raison par r, le nombre des termes par n et leur somme par S.

La différence de deux termes de la progression égale le produit de la raison par la différence des rangs des deux termes.

Si l'on ajoute terme à terme des progressions arithmétiques, on obtient une progression arithmétique dont la raison est la somme algébrique des raisons des progressions données.

La somme de deux termes équidistants des extrêmes est égale à la somme des extrêmes.

La somme des termes d'une progression arithmétique est la moitié du produit du nombre des termes par la somme des extrêmes.

On a donc les formules

$$l - a = (n-1)r, \qquad S = \frac{n(a+l)}{2};$$

et, par suite,

$$S = \frac{2a + (n-1)r}{2}n.$$

Exemple I. — Les nombres triangulaires. — Si l'on dispose des boules en triangles, on forme les nombres triangulaires. En d'autres termes, le $n^{\text{ième}}$ nombre triangulaire P_n^3 est égal à la somme des n premiers nombres. Le double d'un nombre triangulaire de rang quelconque est le produit du nombre qui indique son rang par l'entier suivant. Ainsi

$$P_n^3 = \frac{n(n+1)}{2}.$$

Cette formule se démontre géométriquement de la même manière que l'on démontre que l'aire d'un triangle est la moitié de l'aire d'un parallélogramme. Elle se déduit encore de la somme des termes d'une progression arithmétique de raison $r = 1$; mais le procédé qui sert à calculer cette

somme revient, au fond, à celui qui donne l'aire d'un trapèze comme moitié de celle d'un parallélogramme.

Exemple II. — L'octuple d'un triangulaire, augmenté de l'unité, est un carré. — Ce théorème de DIOPHANTE peut se démontrer géométriquement. En d'autres termes, on a

$$8\frac{n(n+1)}{2}+1=(2n+1)^2.$$

Tout carré impair diminué de 1 est l'octuple d'un triangulaire.

Exemple III. — Aucun triangulaire n'est terminé par les chiffres 2, 4, 9, 7. Car l'octuple plus un serait terminé par 3 ou par 7, ce qui ne peut être le dernier chiffre d'un carré.

Exemple IV. — Le produit de quatre nombres en progression arithmétique, augmenté du bicarré de la raison, est un carré. — En effet

$$a(a+r)(a+2r)(a+3r)+r^4=(a^2+3ar+r^2)^2.$$

Exemple V. — Le produit de quatre entiers consécutifs n'est jamais un carré. — En effet, la différence des carrés de deux entiers consécutifs est au moins égale à 3, et ne peut être égale à $r^4=1$, d'après l'exemple précédent.

Exemple VI. — Tout multiple d'un carré impair est la différence de deux triangulaires. — En effet, on a l'identité

$$a(2x+1)^2=\frac{(2ax+x+a)(2ax+x+a+1)}{2}-\frac{(2ax-x+a-1)(2ax-x+a)}{2}.$$

36. **Les nombres polygonaux.** — Considérons les progressions arithmétiques commençant à 1 et ayant respectivement pour raisons les nombres 1, 2, 3, 4,

$$\begin{array}{llllllll}
1, & 2, & 3, & 4, & 5, & 6, & \ldots, & n,\\
1, & 3, & 5, & 7, & 9, & 11, & \ldots, & 2n-1,\\
1, & 4, & 7, & 10, & 13, & 16, & \ldots, & 3n-2,\\
1, & 5, & 9, & 13, & 17, & 21, & \ldots, & 4n-3.
\end{array}$$

La somme des n premiers termes de ces progressions représente les nombres *triangulaires, carrés, pentagonaux, hexagonaux,* de rang n. En général, le $n^{\text{ième}}$ polygonal P_n^q de q côtés est égal à la somme des n premiers termes de la progression arithmétique commençant à 1, et de raison $(q-2)$. On a donc

$$P_n^q=n+(q-2)\frac{n(n-1)}{2}.$$

Si l'on considère des polygones réguliers, homothétiques par

rapport à l'un des sommets, et contenant 2, 3, 4, ..., n pions à égale distance sur les côtés, on obtient une représentation géométrique du nombre polygonal par l'ensemble des pions.

On démontre facilement par le calcul, ou par une configuration géométrique, les théorèmes suivants :

I. Tout polygonal est égal au nombre qui indique son rang, augmenté d'autant de fois le triangulaire de rang précédent qu'il y a d'unités dans son côté diminué de deux.

II. Tout polygonal est égal au triangulaire de même rang augmenté d'autant de fois le triangulaire précédent qu'il y a d'unités dans son côté diminué de trois.

Il existe une *seconde espèce de nombres polygonaux* de forme plus régulière. On joint le centre d'un polygone régulier à tous les sommets et l'on considère tous les polygones homothétiques par rapport au centre; puis on place des pions à égale distance sur les côtés et au centre, de telle sorte que le premier polygone de q côtés se compose d'un pion au centre, le second de $(1+q)$ pions, le troisième de $(1+q+2q)$ pions, et ainsi de suite. Ainsi le $n^{\text{ième}}$ nombre *polygonal à centre* O_n^q de q côtés a pour expression

$$O_n^q = 1 + q + 2q + \ldots + (n-1)q,$$

c'est à dire

$$O_n^q = 1 + q\frac{n(n-1)}{2}.$$

Si l'on considère un polygonal à centre de $2q$ côtés, et si l'on supprime tous les pions situés d'un côté d'un même diamètre, on voit facilement que l'on peut former avec les pions restants un polygonal de première espèce, de même rang et ayant $(q+2)$ côtés. Ainsi, l'on a la formule

$$O_n^{2q} = 2P_n^{q+2} - 2n + 1.$$

Les exercices suivants se rapportent aux polygonaux de première espèce.

Exemple I. — Le triple de tout pentagonal est un nombre triangulaire dont le rang est le triple moins un du rang du pentagonal.

Exemple II. — Le produit par 24 d'un nombre pentagonal étant augmenté de 1 donne un carré dont le côté est le sextuple moins un du rang du pentagonal.

Exemple III. — Aucun nombre pentagonal ne peut être terminé par l'un des chiffres 3, 4, 8, 9.

Exemple IV. — Tout nombre hexagonal est un triangulaire de côté impair, et réciproquement.

Exemple V. — Aucun nombre hexagonal ne peut être terminé par l'un des chiffres 2, 4, 7, 9.

Exemple VI. — Le nonuple plus un d'un triangulaire est un triangulaire dont le côté est le triple plus un du côté du premier.

Exemple VII. — Le triple plus un d'un octogonal est un carré dont le côté est le triple moins un du côté de l'octogonal.

Exemple VIII. — Le double plus un d'un décagonal est un triangulaire dont le rang est le quadruple moins deux de celui du décagonal.

Exemple IX. — Aucun décagonal ne peut être terminé par l'un des chiffres 3, 4, 8, 9.

Exemple X. — Construire le tableau des dix premiers nombres polygonaux ayant dix côtés au plus.

Exemple XI. — Étant donné un nombre, trouver de combien de manières il peut être polygonal (FERMAT). — Il suffit de diviser le nombre donné par les triangulaires successifs, en ne conservant que les divisions dans lesquelles le reste est égal au triangulaire de rang précédent.

Exemple XII. — Trouver un nombre qui soit polygonal autant de fois qu'on voudra (FERMAT). — Le problème se ramène à la détermination d'un nombre qui, divisé par des nombres donnés, donne des restes donnés. La solution complète de ce problème rentre dans la théorie des congruences du premier degré qui sera exposée plus loin.

Pour plus de détails, voir notre article intitulé : *L'Arithmétique en boules* (n° 696 de *La Nature*).

37. Sommation des factorielles. — On appelle *factorielle* le produit de facteurs en progression arithmétique. Les factorielles consécutives donnent lieu à des formules importantes concernant les sommes

$$\begin{aligned}
\Sigma_1 &= a + b + \ldots + k + l,\\
\Sigma_2 &= ab + bc + \ldots + hk + kl,\\
\Sigma_3 &= abc + bcd + \ldots + ghk + hkl,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Posons, pour abréger, $(a - r) = \alpha$ et $(l + r) = \lambda$; on a les égalités

$$\begin{aligned}
ab - \alpha a &= 2r.a,\\
bc - ab &= 2r.b,\\
cd - bc &= 2r.c,\\
&\ldots\ldots\ldots\ldots,\\
l\lambda - kl &= 2r.l;
\end{aligned}$$

en ajoutant et en simplifiant, on trouve

$$l\lambda - \alpha a = 2r.\Sigma_1.$$

En partant des égalités

$$\begin{aligned} abc \quad &- \alpha ab \quad = 3r.ab, \\ abcd \quad &- \alpha abc \quad = 4r.abc, \\ abcde &- \alpha abcd = 5r.abcd, \\ &\dots\dots\dots\dots, \end{aligned}$$

on trouve, de même, la série des formules

$$\begin{aligned} 2r.\Sigma_1 &= \quad l\lambda - \alpha a, \\ 3r.\Sigma_2 &= \quad kl\lambda - \alpha ab, \\ 4r.\Sigma_3 &= \quad hkl\lambda - \alpha abc, \\ 5r.\Sigma_4 &= ghkl\lambda - \alpha abcd, \\ &\dots\dots\dots\dots \end{aligned}$$

Exemple I. — Démontrer les formules

$$\begin{gathered} 1 + 3 + 5 + \dots \qquad + (2n - 1) = n^2, \\ 1.3 + 3.5 + \dots + (2n-1)(2n+1) = \tfrac{1}{3}n(4n^2 + 6n - 1), \\ 1.3.5 + \dots + (2n-1)(2n+1)(2n+3) = n(2n^3 + 8n^2 + 7n - 2). \end{gathered}$$

38. Les nombres figurés. — Pour la progression des nombres entiers commençant à l'unité, on a $\alpha = 0$ et $r = 1$. En supposant que la progression contienne successivement p, $(p+1)$, $(p+2)$, ... termes, on a

$$\begin{gathered} 1 + 2 + 3 + \dots + p = \tfrac{1}{2}p(p+1), \\ 1.2 + 2.3 + 3.4 + \dots + p(p+1) = \tfrac{1}{3}p(p+1)(p+2), \\ 1.2.3 + 2.3.4 + \dots + p(p+1)(p+2) = \tfrac{1}{4}p(p+1)(p+2)(p+3), \\ \dots\dots\dots\dots\dots\dots\dots\dots \end{gathered}$$

On vérifie immédiatement *a posteriori* la formule qui résume les précédentes

$$(1) \qquad \sum_{x=1}^{x=p} x(x+1)\dots(x+q-2) = \frac{1}{q}\,p(p+1)\dots(p+q-1),$$

en montrant que, si la formule est exacte pour les premières valeurs de p, elle a lieu encore pour la valeur suivante.

En effet, q restant fixe, la formule a lieu pour $p = 1$; mais, lorsqu'on remplace p par $(p+1)$, le second membre augmente de

$$\frac{(p+1)(p+2)\ldots(p+q-1)}{q}[(p+q)-p];$$

c'est précisément, après simplification, l'accroissement du premier membre.

Nous avons vu que le nombre triangulaire de rang p est égal à la somme des p premiers entiers. Autrefois, on désignait encore les nombres triangulaires sous l'appellation de *nombres figurés du second ordre*, ou à *deux dimensions*. En général, on appelle *nombre figuré* F_p^q *d'ordre* q (ou à q dimensions) le nombre égal à la somme des p premiers nombres figurés d'ordre $(q-1)$; on a donc, par définition,

$$F_p^q = F_1^{q-1} + F_2^{q-1} + F_3^{q-1} + \ldots + F_p^{q-1},$$

et, par suite,

$$(2) \qquad F_p^q = F_{p-1}^q + F_p^{q-1}.$$

Si l'on construit, par additions successives, le Tableau des nombres figurés *naturels, triangulaires, pyramidaux*, ..., on obtient (*fig.* 27):

Fig. 27.

F^0	F^1	F^2	F^3
1	1	1	1
1	2	3	4
1	3	6	10
1	4	10	20
1	5	15	35
.	.	..	..

Table des nombres figurés.

D'ailleurs, la formule (1) donne, pour le calcul direct,

$$(3) \qquad F_p^q = \frac{p(p+1)\ldots(p+q-1)}{q!}.$$

Si l'on baisse d'une ligne la colonne des entiers F^1, de deux

lignes celle des triangulaires F^2, de trois lignes celle des pyramidaux F^3, et ainsi de suite, le Tableau des nombres figurés devient le triangle arithmétique de Pascal, et l'on a

$$(4) \qquad F_p^q = C_{p+q-1}^q.$$

Les résultats qui précèdent ont été trouvés par FERMAT, en 1636, d'après la méthode inductive. Il s'exprime ainsi dans ses Notes sur DIOPHANTE, à la suite de la Proposition IX du Livre des *Polygones* : « Propositionem pulcherrimam et mirabilem quam nos invenimus hoc in loco sine demonstratione opponemus. In progressione naturali quæ ab unitate sumit exordium quilibet numerus in proxime majorem facit duplum sui trianguli, in triangulum proxime majoris facit triplum suæ pyramidis, in pyramidem proxime majoris facit quadruplum sui triangulotrianguli, et sic uniformi et generali in infinitum methodo. Nec existimo pulchrius aut generalius in numeris posse dari theorema cujus demonstrationem margini inserere nec curat nec vacat. »

Postérieurement, FERMAT écrit à PASCAL le 29 août 1654 : « Nos coups fourrés continuent toujours, et je suis aussi bien que vous dans l'admiration de quoi nos pensées s'ajustent si exactement, qu'il me semble qu'elles aient pris une même route et fait un même chemin : Vos derniers Traités du *Triangle arithmétique et de son application* en sont une preuve authentique; et, si mon calcul ne me trompe, votre onzième conséquence courait la poste de Paris à Toulouse, pendant que ma proposition des nombres figurés, qui, en effet, est la même, allait de Toulouse à Paris. Je n'ai garde de faillir, tandis que je rencontrerai de cette sorte, et je suis persuadé que le vrai moyen pour l'empêcher de faillir est celui de concourir avec vous; mais, si j'en disais davantage, la chose tiendrait du compliment, et nous avons promis de bannir cet ennemi des conversations douces et aisées. »

Voir le *Traité des ordres numériques* de PASCAL.

39. Piles d'obus et piles de boulets. — La *pile d'obus* est prismatique et se compose de p tranches triangulaires. Le nombre des obus qu'elle contient est le produit par p du triangulaire correspondant.

La *pile de boulets à base triangulaire*, ayant n boulets au côté, contient un nombre de boulets T_n égal à la somme des n premiers nombres triangulaires; c'est le nombre pyramidal de rang n,

$$F_n^3 = T_n = \frac{1.2}{2} + \frac{2.3}{2} + \ldots + \frac{n(n+1)}{2},$$

c'est-à-dire

$$T_n = \frac{n(n+1)(n+2)}{1.2.3}.$$

La *pile de boulets à base carrée,* ayant n boulets au côté, contient un nombre de boulets Q_n égal à la somme des n premiers carrés. On peut la considérer comme formée de deux piles triangulaires T_n et T_{n-1}; on a, en effet, pour chaque tranche,

$$n^2 = \frac{n(n+1)}{2} + \frac{(n-1)n}{2};$$

par suite, en remplaçant n par $1, 2, 3, \ldots, n$, et faisant la somme, on voit que Q_n est la somme des pyramidaux de rangs n et $(n-1)$. On a

$$Q_n = \frac{n(n+1)(2n+1)}{6}.$$

Pour les trois piles, le nombre des projectiles est égal au nombre des projectiles d'une face triangulaire, multiplié par le tiers du nombre des projectiles contenus dans trois arêtes parallèles partant des sommets de cette face.

Cette formule subsiste pour la pile quadrangulaire, que l'on peut considérer comme la réunion d'une pile à base carrée et d'une pile prismatique.

Pour plus de détails, voir notre article intitulé : *L'Arithmétique en bâtons* (n° 697 de *La Nature*).

Exemple I. — On a les inégalités

$$n^3 < 6T_n < (n+1)^3,$$
$$n^3 < 3Q_n < (n+1)^3,$$

qui permettent de déterminer n, connaissant T_n ou Q_n, au moyen de la Table des cubes (*Algèbre* d'EULER).

Exemple II. — Le nombre des boulets d'une pile à base carrée de rang n est le quart du nombre des boulets d'une pile à base triangulaire de rang $2n$.

Exemple III. — Le nombre des boulets contenus dans l'ensemble des n premières piles triangulaires est égal au $n^{\text{ième}}$ nombre triangulo-triangulaire

$$F_n^4 = \frac{n(n+1)(n+2)(n+3)}{1.2.3.4}.$$

Exemple IV. — Le nombre des boulets contenus dans l'ensemble des n premières piles à base carrée est la somme des triangulo-triangulaires de rangs n et $(n-1)$, ou

$$F^4_{n-1} + F^4_n = \frac{n(n+1)^2(n+2)}{12}.$$

Exemple V. — Démontrer directement la formule qui donne le nombre des boulets d'une pile à base rectangulaire.

Exemple VI. — Trouver le nombre des projectiles qui se trouvent sur la surface latérale ou totale d'une pile. — Huit cas.

Exemple VII. — Nombre des boulets d'une pile tronquée à bases parallèles. — Quatre cas.

Exemple VIII. — Trouver la somme des n premiers polygonaux de q côtés et de première espèce. — On a

$$P^q_1 + P^q_2 + \ldots + P^q_n = \frac{n(n+1)}{2} + (q-2)\frac{(n-1)n(n+1)}{6}.$$

Pour $q = 3$ et pour $q = 4$, on retrouve les expressions de T_n et de Q_n.

Exemple IX. — Trouver la somme des n premiers polygonaux de q côtés et de seconde espèce. — On a

$$Q^q_1 + Q^q_2 + \ldots + Q^q_n = n + q\frac{(n-1)n(n+1)}{6}.$$

Lorsque $q = 6$, on trouve n^3 pour la pile hexagonale de n pions sur le côté de la base.

Exemple X. — Trouver la somme des polygonaux de rang n et de première espèce, dont les côtés sont 3, 4, 5, ..., q. — On a

$$P^3_n + P^4_n + \ldots + P^q_n = n(q-2) + \frac{n(n-1)}{2}\frac{(q-2)(q-1)}{2}.$$

Exemple XI. — Trouver la somme des polygonaux de rang n et de seconde espèce, dont les côtés sont 3, 4, 5, ..., q. — On a

$$Q^3_n + Q^4_n + \ldots + Q^q_n = (q-2) + \frac{n(n-1)}{2}\left[\frac{q(q+1)}{2} - 3\right].$$

Exemple XII. — Trouver la somme de tous les polygonaux des n premiers rangs et dont les côtés sont 3, 4, 5, ..., q. — Deux cas.

Exemple XIII. — Dans un système de numération de base B, la somme des chiffres de tous les nombres n'ayant pas plus de n chiffres est

$$\tfrac{1}{2}nB^n(B-1).$$

Le produit des chiffres significatifs de tous ces nombres est égal à la puissance de la factorielle $(B-1)!$ qui a pour exposant nB^{n-1}.

40. Binôme de Newton. — La théorie des nombres figurés conduit au triangle arithmétique de PASCAL et à la formule appelée *binôme de* NEWTON.

Si l'on multiplie le polynôme

$$F = a + bx + cx^2 + \ldots + kx^{n-1} + lx^n$$

par $(1 + x)$, et si l'on n'écrit que les coefficients de F et ceux du produit P, on trouve

$$\begin{array}{llllllll} \text{pour F.....} & a, & b, & c, & \ldots, & k, & l; & \\ \text{pour P.....} & a, & a+b, & b+c, & \ldots, & h+k & k+l, & l, \end{array}$$

comme dans la multiplication d'un nombre par 11 (n° 18, *Ex. I*); par conséquent, ces coefficients se calculent comme dans un Tableau de sommes (n° 5).

En particulier, les coefficients des puissances successives de $(1 + x)$ produisent le triangle arithmétique de PASCAL. On a donc le développement

$$(1 + x)^p = 1 + C_p^1 x + C_p^2 x^2 + \ldots + C_p^q x^q + \ldots + C_p^p x^p;$$

d'ailleurs, si l'on remplace dans la formule (4) du n° 38 le nombre p par $(p - q + 1)$, il vient, en tenant compte de la formule (3) qui donne l'expression générale des nombres figurés,

$$C_p^q = F_{p-q+1}^q = \frac{p(p-1)\ldots(p-q+1)}{1.2.3\ldots q}.$$

On a donc le développement

$$(1+x)^p = 1 + \frac{p}{1}x + \frac{p(p-1)}{1.2}x^2 + \ldots + \frac{p(p-1)\ldots(p-q+1)}{1.2.3\ldots q}x^q + \ldots + x^p.$$

On peut vérifier *a posteriori* l'exactitude de ce développement, en faisant voir que, si cette formule est une identité pour une valeur entière et positive de l'exposant p, elle a lieu encore pour l'exposant $(p + 1)$.

En remplaçant x par $(b : a)$ et en multipliant les deux membres par a^p, on a la formule

$$(a + b)^p = a^p + \frac{p}{1}a^{p-1}b + \frac{p(p-1)}{1.2}a^{p-2}b^2 + \ldots + b^p.$$

41. Propriétés des coefficients du développement de $(1+x)^p$. — Les coefficients de ce développement, que nous désignerons souvent, pour abréger, par $1, p_1, p_2, \dots, p_p$, sont en nombre $(p+1)$.

On a d'ailleurs

$$p_q = C_p^q = \frac{p!}{q!(p-q)!} = C_p^{p-q} = p_{p-q}.$$

Les coefficients à égale distance des extrêmes sont égaux; ils vont en croissant jusqu'au milieu du développement.

La somme des coefficients est égale à 2^p et la somme alternée est nulle, ainsi qu'on le voit en remplaçant x par $+1$ et par -1.

On en déduit les sommes des coefficients de deux en deux.

$$1 + p_2 + p_4 + p_6 + \dots = 2^{p-1},$$
$$p_1 + p_3 + p_5 + \dots = 2^{p-1}.$$

Les coefficients étant entiers, C_p^q est entier, quelles que soient les valeurs des nombres entiers positifs p et q; par conséquent, *le produit de q nombres entiers consécutifs est divisible par le produit des q premiers nombres entiers.* D'ailleurs C_p^q est nul pour $q > p$.

Exemple I. — *Produit des coefficients du binôme.* — En partant de l'expression

$$C_p^q = \frac{p!}{q!(p-q)!} = C_p^{p-q},$$

on trouve facilement, pour le produit des coefficients du développement de $(1+x)^p$, la valeur

$$\frac{(p!)^{p-1}}{[1!\,2!\,3!\dots(p-1)!]^2}.$$

Exemple II. — *Somme alternée des q premiers coefficients.* — En se reportant au n° 13 (*Ex. II*), on a

$$1 - C_p^1 + C_p^2 - C_p^3 + \dots + (-1)^q C_p^q = (-1)^q C_{p-1}^q.$$

Il n'existe pas de formule simple pour la somme des q premiers coefficients du développement de $(1+x)^p$.

Exemple III. — Démontrer les formules suivantes dues à M. Delannoy.

$$p + (p-2)C_p^1 + (p-4)C_p^2 + \dots + (p-2q+2)C_p^{q-1} = qC_p^q,$$
$$p - (p-2)C_p^1 + \dots + (-1)^{q-1}(p-2q+2)C_p^{q-1} = (-1)^{q-1}\frac{q(p-2q+1)}{p-1}C_p^q.$$

CHAPITRE VI.

L'ANALYSE COMBINATOIRE.

---

42. **Permutations.** — Ce sont les manières de disposer n objets différents en ligne droite et, plus particulièrement, les manières diverses d'écrire la somme ou le produit de n nombres inégaux deux à deux. En désignant le nombre de ces manières par P_n, on a

$$P_n = nP_{n-1} \quad \text{et} \quad P_n = 1.2.3 \ldots n.$$

En d'autres termes, *le nombre des permutations de n objets différents est égal au produit des n premiers nombres.* On désigne encore ce produit par $n!$ que l'on appelle *factorielle n.*

Lorsque l'on remplace, dans une suite d'objets, chacun d'eux par le suivant, on fait une *permutation circulaire.* Le nombre des permutations de n objets différents, placés sur une circonférence, est égal à P_{n-1} ou $(n-1)!$

Formation du Tableau des permutations de n nombres dans l'ordre numérique, ou de n lettres dans l'ordre alphabétique. — Connaissant une permutation, trouver son rang dans le Tableau. — Inversement, écrire une permutation dont le rang est donné.

L'analyse combinatoire a été imaginée par FERMAT et PASCAL pour obtenir la solution de problèmes sur le Calcul des probabilités. Dans son *Traité du Triangle arithmétique,* PASCAL en donne deux applications; l'une est intitulée : *Usage du triangle arithmétique pour les combinaisons,* et l'autre : *Usage du triangle arithmétique pour déterminer les partis qu'on doit faire entre deux joueurs qui jouent en plusieurs parties.*

Lorsque la permutation des lettres d'un mot, ou d'une phrase, forme un nouveau mot, ou une nouvelle phrase, la permutation prend le nom d'*anagramme.* Ainsi les mots *logarithme* et *algorithme* sont formés des mêmes lettres dans un ordre différent. PASCAL, dans les *Pensées,* s'est caché sous le pseudonyme de SALOMON DE TULTIE, anagramme de LOUIS DE MONTALTE, nom sous lequel il fit paraître les *Lettres provinciales.*

Exemple I. — Calculer le nombre des permutations de n objets pour toutes les valeurs entières de n jusqu'à 25.

1.2.3. ... n ou $n!$	n
1	1
2	2
6	3
24	4
120	5
720	6
5040	7
40320	8
3 62880	9
36 28800	10
399 16800	11
4790 01600	12
62270 20800	13
8 71782 91200	14
130 76743 68000	15
20922 78988 80000	16
35568 74280 96000	17
6 40237 37057 28000	18
121 64510 04088 32000	19
2432 90200 81766 40000	20
51090 94217 17094 40000	21
11 24000 72777 76076 80000	22
258 52016 73888 49766 40000	23
6204 48401 73323 94393 60000	24
1 55112 10043 33098 59840 00000	25

Les permutations des 25 premiers nombres.

On voit ainsi que le nombre des permutations de n objets augmente rapidement avec n. Pour des valeurs plus grandes de n, on ne calcule habituellement que le nombre des chiffres et les premiers chiffres, au moyen d'une formule donnée par STIRLING.

Exemple II. — Trouver le nombre des manières de permuter un mot formé de n consonnes et de n voyelles distinctes, de telle sorte qu'il n'y ait pas deux voyelles ou deux consonnes consécutives. — On trouve $2(P_n)^2$, et ainsi pour un mot composé de cinq consonnes et de cinq voyelles, toutes distinctes, ce nombre est égal à 28800, tandis que le nombre de toutes les permutations est $P_{10} = 3\,628\,800$.

Exemple III. — On permute les chiffres 1, 2, 3, 4, 5 de toutes les manières possibles; trouver la somme des nombres formés par ces permutations dans le système décimal.

On prend la somme des nombres donnés par une permutation et par la *permutation complémentaire;* on trouve ainsi, puisque la somme des nombres de deux permutations complémentaires, telles que

$$\begin{array}{r} 24513 \\ 42153 \\ \hline 66666 \end{array}$$

est constante, que la somme cherchée est la moitié du produit de P_5 par le nombre 66666.

43. Permutations figurées. — Ce sont les dispositions de n jetons sur les cases d'un échiquier de n^2 cases, de telle sorte qu'il n'y ait pas deux jetons sur une même ligne $\rightarrow$ ou sur une même colonne $\downarrow$. Ces dispositions correspondent au *problème des tours au jeu d'échecs.*

A toute permutation de n nombres correspond une permutation figurée, et inversement; nous trouverons l'application des permutations figurées dans la théorie des déterminants.

La *fig.* 28 représente les permutations figurées de quatre éléments 1, 2, 3, 4; elles sont rangées dans l'ordre numérique, d'après la permutation correspondante placée au-dessous de chacune d'elles. Les cases ombrées figurent les jetons.

Nous montrerons plus loin, au Chapitre VIII, que cette représentation des permutations, qui constitue un ensemble important des théories de l'*Arithmétique de position,* trouve encore une intéressante application dans les produits des sommes de quatre carrés, et dans la théorie des factorielles.

Exemple I. — Dans toute permutation figurée, le nombre des jetons situés sur les cases de couleur opposée à celle d'un coin de l'échiquier est toujours pair (*voir* n° 8).

En effet, soient

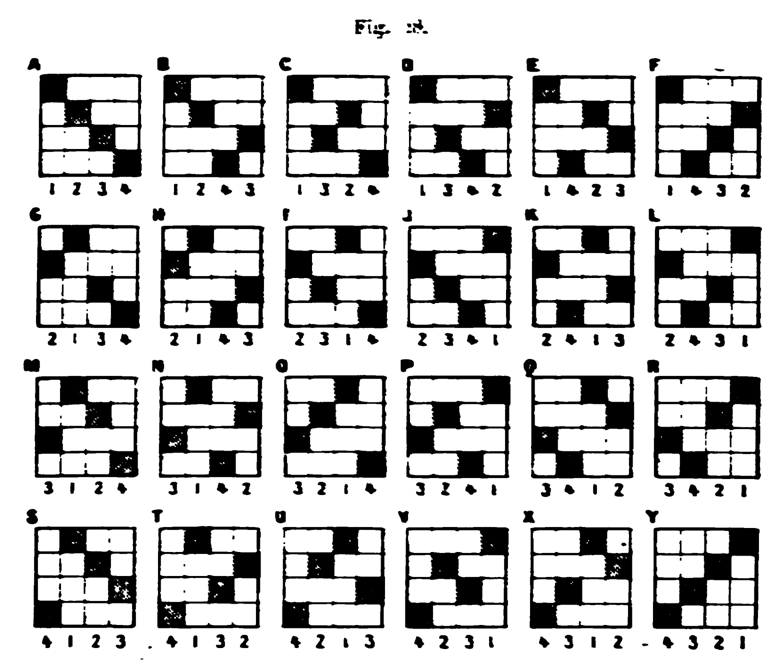
$$(1, y_1), \quad (2, y_2), \quad (3, y_3), \quad \ldots, \quad (n, y_n),$$

les coordonnées des jetons d'une permutation figurée $y_1 y_2 y_3 \ldots y_n$, en prenant le coin de coordonnées (1, 1) pour origine. La somme de toutes les coordonnées

$$(1 + y_1) + (2 + y_2) + (3 + y_3) + \ldots + (n + y_n),$$

vant évidemment le double de la somme des n premiers nombres et, par suite, un nombre pair. D'autre part, si l'on supprime les parenthèses à

Fig. 28.



Les permutations figurées de quatre éléments.

somme paire, qui correspondent à des jetons posés sur des cases de même couleur que la case (1.1), il reste un total pair. Par suite, les parenthèses à somme impaire, qui correspondent aux jetons placés sur des cases de couleur opposée à celle du coin (1.1), forment un nombre pair; elles sont donc en nombre pair.

Exemple II. — Trouver le nombre G_n des permutations des n premiers chiffres, dans lesquelles la somme des chiffres à égale distance des extrêmes est la même. En d'autres termes, trouver le nombre des permutations figurées qui sont symétriques par rapport au centre de l'échiquier.

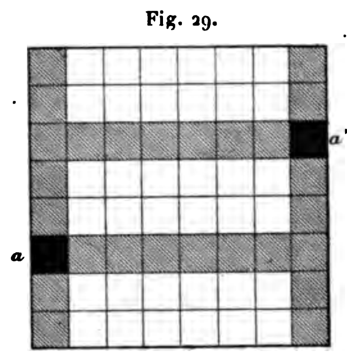
Si n est impair, il y a une tour au centre de l'échiquier, et, en supprimant la ligne et la colonne du milieu, on obtient un échiquier dont le côté est $(n-1)$. On a ainsi

$$G_{2n+1} = G_{2n}.$$

Soit (*fig.* 29) un échiquier pair de côté $2n$; la position d'un jeton a dans la première colonne donne la position d'un jeton a' dans la dernière co-

lonne; en supprimant les lignes et les colonnes qui contiennent a et a', il reste un ensemble de cases qui correspond à un échiquier de $(2n-2)$

Fig. 29.



Permutations symétriques.

cases de côté. Mais a peut occuper $2n$ places dans la première colonne; par suite

$$G_{2n} = 2n\,G_{2n-2};$$

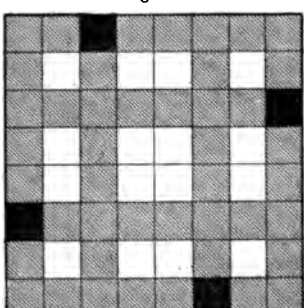
d'où l'on déduit

$$G_{2n+1} = G_{2n} = 2^n . n!$$

Exemple III. — Déterminer le nombre R_n des permutations figurées qui coïncident avec elles-mêmes en faisant tourner l'échiquier d'un quart de tour (*fig.* 30).

La permutation est symétrique par rapport au centre de l'échiquier, car

Fig. 30.



Permutations tournantes.

elle coïncide avec elle-même par rotation de deux quarts de tour. On a, puisque les jetons vont par quatre, sauf au centre,

$$R_{4n+1} = R_{4n}, \qquad \text{et} \qquad R_{4n+3} = R_{4n+2} = 0;$$

puis, comme précédemment, en observant que le jeton ne peut être placé dans un coin de l'échiquier,

$$R_{4n} = (4n - 2)\, R_{4n-4};$$

par suite

$$R_{4n} = 2.6.10.\ \ldots\ (4n - 2).$$

Exemple IV. — De combien de manières peut-on effectuer le produit de n facteurs distincts, en supposant que tous les produits diffèrent des facteurs et diffèrent entre eux ?

Soit O_n ce nombre de manières; le nombre de multiplications à faire dans chacune des manières est toujours $(n - 1)$. On a d'abord, pour deux facteurs a et b, les multiplications ab et ba; donc $O_2 = 2$.

Prenons un troisième facteur c; on peut le combiner comme multiplicateur ou comme multiplicande avec le produit effectué, ce qui donne

$$c(ab) \quad \text{et} \quad (ba)c;$$

mais on peut aussi faire intervenir le nombre c, pendant la multiplication, de quatre manières :

$$acb, \quad cab, \quad bca, \quad cba;$$

on a donc $O_3 = 6\,O_2$. Prenons un quatrième facteur d et combinons-le avec l'un des O_3 produits entièrement effectués, abc par exemple. On a deux manières distinctes :

$$d(abc) \quad \text{et} \quad (abc)d;$$

mais, si l'on introduit le facteur d pendant l'opération, abc exige deux multiplications. Donc, en faisant intervenir d dans l'intervalle de la multiplication de a par (bc), il y a quatre manières :

$$ad(bc), \quad da(bc), \quad a(dbc), \quad a(bdc),$$

et autant pour la multiplication de (bc) par a; en tout dix manières. On a donc

$$O_4 = 10\,O_3.$$

Désignons par M une des manières employées pour obtenir le produit de $(n - 1)$ facteurs, et introduisons le nouveau facteur f. Celui-ci peut se combiner comme multiplicande ou comme multiplicateur, ce qui donne les deux cas Mf et fM; mais, si on l'introduit avant d'avoir effectué le produit M, il y a $(n - 2)$ multiplications dont chacune donne quatre manières; donc en tout

$$2 + 4(n - 2) \quad \text{ou} \quad 4n - 6;$$

par suite

$$O_n = (4n - 6)\, O_{n-1},$$

et

$$O_n = 2.6.10\ \ldots\ (4n - 6) = 2^{n-1}.1.3.5\ \ldots\ (2n - 3).$$

Cette démonstration est due à O. RODRIGUES; mais le résultat précédent est de M. CATALAN (*Journal de Liouville*, 1[re] série, t. III et VI).

44. Permutations avec répétition. — Ce sont les diverses manières de disposer n objets en ligne droite, ces objets n'étant pas tous distincts. Par exemple, si α lettres sont égales à a, si β lettres sont égales à b, ..., λ lettres à l, avec la condition

$$\alpha + \beta + \ldots + \lambda = n,$$

le nombre des permutations avec répétition est

$$\frac{n!}{\alpha!\,\beta!\ldots\lambda!}.$$

Exemple I. — De combien de manières peut-on effectuer le produit de n facteurs égaux ou inégaux?

Si α facteurs sont égaux à a, β à b, γ à c, ..., en désignant par a, b, c, ... des facteurs quelconques inégaux, il faut diviser

$$O_n = 2^{n-1}.1.3.5.\ldots(2n-3),$$

par le produit des factorielles

$$\alpha!\,\beta!\,\gamma!\,\ldots$$

Exemple II. — De combien de manières peut-on remplacer le produit de n facteurs par des produits de deux facteurs dans le cas de n pair, et par des produits de deux facteurs et d'un seul, dans le cas de n impair?

Exemple III. — De combien de manières peut-on décomposer un produit de $3n$ facteurs en n produits de trois facteurs?

On trouve

$$\frac{(3n)!}{(3!)^n.\,n!}.$$

45. Arrangements simples. — Les arrangements simples de p objets distincts, pris q à q, sont les manières de disposer en ligne droite q de ces objets, de telle sorte que deux dispositions diffèrent soit par le *choix*, soit par l'*ordre* des objets.

En désignant leur nombre par A_p^q, on déduit ces arrangements des arrangements A_p^{q-1}, en écrivant successivement à la suite de ces derniers les $(p-q+1)$ lettres qui n'y entrent pas

$$A_p^q = (p-q+1)\,A_p^{q-1};$$

par suite,

$$A_p^q = p(p-1)(p-2)\ldots(p-q+1).$$

Ainsi, *le nombre des arrangements simples de p objets, pris q à q, est le produit des q nombres entiers décroissants à partir de p.*

Si $p = q$, on retrouve les permutations; si $p < q$, on a $A_p^q = 0$, conformément à la définition.

Si l'on exprime, de deux manières différentes, le nombre de fois qu'une lettre a entre dans le tableau des arrangements à une place déterminée, à la première par exemple, on a encore la formule de récurrence

$$A_p^q = p A_{p-1}^{q-1}.$$

Exemple I. — Former les arrangements simples de p lettres, prises q à q, en suivant l'ordre alphabétique.

Connaissant un arrangement simple, trouver son rang dans le tableau.

Inversement, écrire un arrangement simple de rang donné.

Exemple II. — Trouver la somme de tous les nombres du système décimal qui n'ont pas plus de cinq chiffres, et formés seulement des chiffres 0, 1, 2, 3, 4, les chiffres ne pouvant être répétés.

Exemple III. — Décomposer le tableau des arrangements simples de p lettres, prises q à q, d'après la considération d'une lettre a.

Exemple IV. — Décomposer le tableau des arrangements simples de p lettres, prises q à q, d'après la considération de deux lettres a et b.

46. Arrangements complets. — Les arrangements complets de p objets, pris q à q, sont les manières de disposer en ligne droite q de ces objets, ces objets pouvant être répétés jusqu'à q fois, mais de telle sorte que deux dispositions diffèrent soit par le *choix*, soit par l'*ordre* de ces objets.

En désignant leur nombre par B_p^q, on a

$$B_p^q = p B_p^{q-1} \qquad \text{et} \qquad B_p^q = p^q.$$

Ainsi, *le nombre des arrangements complets de p objets, pris q à q, est le produit de q nombres égaux à p.*

Si l'on écrit tous les nombres du système de base p jusqu'à q chiffres, en complétant par des zéros à la gauche tous ceux qui ont moins de q chiffres, et en commençant par 000...0, on forme les arrangements complets de p chiffres pris q à q.

Exemple I. — Connaissant un arrangement complet de p chiffres pris q à q, trouver son rang et inversement.

Exemple II. — Trouver la somme de tous les nombres du système décimal qui n'ont pas plus de q chiffres.

Exemple III. — Décomposer le tableau des arrangements complets de p lettres, prises q à q, d'après la considération d'une lettre a.

Exemple IV. — Décomposer le tableau des arrangements complets de p lettres, prises q à q, d'après la considération de deux lettres a et b.

47. Combinaisons simples. — Les *combinaisons* simples de p objets, pris q à q, sont les groupes que l'on peut former avec q de ces objets, de telle sorte que deux groupes diffèrent par le *choix* et non par l'*ordre* des objets. Ainsi

les *Permutations* P_q ne diffèrent que par l'ordre,
les *Combinaisons* C_p^q » » le choix,
les *Arrangements* A_p^q diffèrent par l'ordre ou par le choix.

On a la formule

$$A_p^q = P_q . C_p^q,$$

et, par suite,

$$C_p^q = \frac{p(p-1)\ldots(p-q+1)}{1.2.3\ldots q}.$$

Ainsi, *le nombre des combinaisons simples de p objets, pris q à q, est le produit des q nombres entiers décroissants à partir de p, divisé par le produit des q premiers nombres.*

On peut encore écrire

$$C_p^q = \frac{p!}{q!(p-q)!} = C_p^{p-q}.$$

A toute combinaison C_p^q en correspond une autre, *complémentaire.*

Si l'on suppose que les objets sont des lettres que l'on peut ranger dans chaque combinaison, suivant l'ordre alphabétique, et si l'on observe que le tableau des combinaisons est symétrique par rapport à toutes les lettres qui y entrent, on voit que

le nombre des lettres du tableau est........... $q\,C_p^q$;
le nombre de fois que a s'y trouve est......... $\frac{q}{p}\,C_p^q$;
le nombre des combinaisons contenant a est... C_{p-1}^{q-1}.

On a donc la formule

$$q\,C_p^q = p\,C_{p-1}^{q-1};$$

d'où l'on déduit encore l'expression de C_p^q.

Enfin on a la formule

$$qC_p^q = (p-q-1)\,C_{p-1}^q.$$ Not true

que l'on démontre en ajoutant à chacune des combinaisons du tableau C_{p-1}^q, chacune des $(p-q-1)$ lettres qui n'y entrent pas et en observant que l'on reproduit ainsi q fois le tableau C_p^q.

Exemple I. — De combien de manières peut-on appliquer quatre, au plus, des sept couleurs du spectre solaire, sur les faces d'un tétraèdre régulier ?

Pour quatre couleurs distinctes.......	$2C_7^4$ ou	70
» trois » »	$3C_7^3$ »	105
» deux » »	$3C_7^2$ »	63
» une » »	C_7^1 »	7
En tout.................		245

Exemple II. — Démontrer directement que le nombre de toutes les combinaisons possibles de p lettres est égal à $2^p - 1$. — En effet, prenons, par exemple, quatre lettres a, b, c, d; formons toutes les combinaisons possibles de ces quatre lettres; ajoutons-y l'unité; nous formons le tableau de gauche, dont le nombre des combinaisons est, en comptant 1, égal à 2^4. Ajoutons une lettre e, nous formons le tableau de droite. Ainsi le nombre des combinaisons possibles de cinq lettres est le double de celui de quatre lettres, et ainsi de suite.

Fig. 31.

1,	*e*.
a, *b*, *c*, *d*,	*ae*, *be*, *ce*, *de*,
ab, *ac*, *ad*, *bc*, *bd*, *cd*.	*abe*, *ace*, *ade*, *bce*, *bde*, *cde*.
abc, *abd*, *acd*, *bcd*,	*abce*, *abde*, *acde*, *bcde*,
abcd.	*abcde*.

Combinaisons de quatre et de cinq lettres.

On peut donner une autre démonstration fondée sur la considération du système de la numération binaire. Si l'on considère les unités des différents ordres jusqu'au $n^{ième}$ comme des objets différents, tous les nombres du système binaire ayant n chiffres au plus représentent, après suppression du zéro, toutes les combinaisons de n objets pris un à un, deux à deux, ..., jusqu'à n, c'est-à-dire tous les nombres qui ont 1, 2, 3, ..., chiffres significatifs dans le système binaire. Le nombre total des combinaisons est donc égal au nombre du système binaire formé par n fois le chiffre 1 ou $2^n - 1$. Le *Jekim*, boulier chinois de Fo-CHI, est une représentation sensible de cette démonstration.

De même, le nombre de toutes les combinaisons de n objets distincts pris un à un, deux à deux, trois à trois, ..., en supposant que chaque objet puisse être pris deux fois, est égal à $3^n - 1$, comme cela résulte de la considération du système de la numération ternaire, ou du boulier correspondant. Et ainsi de suite.

Exemple III. — De combien de manières peut-on décomposer le produit $N = abc\ldots l$, de n facteurs, en un produit de deux facteurs?

C'est la moitié du nombre des combinaisons de n objets pris un à un, deux à deux, ..., n à n, ou 2^{n-1}, en comptant le produit $1.N$, et en considérant comme une seule manière le produit pq et le produit qp.

Exemple IV. — Les combinaisons du tableau C_p^q étant rangées suivant l'ordre alphabétique, trouver le rang d'une combinaison donnée. Inversement, écrire la combinaison de rang donné.

Exemple V. — Même question pour le tableau alphabétique de toutes les combinaisons possibles de p lettres, chacune d'elles ne pouvant être prise plus d'une fois.

48. Addition des combinaisons simples. — On a la formule

$$C_p^q = C_{p-1}^q + C_{p-1}^{q-1}, \quad (1)$$

qui correspond à la loi de formation du triangle arithmétique, et, puisque les deux premières lignes du tableau des nombres de combinaisons et du triangle sont les mêmes, on en déduit que les tableaux sont identiques.

Exemple I. — Vérifier la formule (1) par l'expression de C_p^q.

Exemple II. — Décomposer le tableau C_p^q par la considération de deux lettres a et b.

Combinaisons ne contenant ni a ni b	....	C_{p-2}^q
Combinaisons contenant a et non b	....	C_{p-2}^{q-1}
» » b et non a	....	C_{p-2}^{q-1}
» » a et b	....	C_{p-2}^{q-2};

on a donc la formule

$$C_p^q = C_{p-2}^q + 2C_{p-2}^{q-1} + C_{p-2}^{q-2},$$

que l'on peut vérifier par l'expression de C_p^q ou déduire de la formule (1), par l'addition des égalités

$$C_{p-1}^q = C_{p-2}^{q-1} + C_{p-2}^{q-1},$$
$$C_{p-1}^{q-1} = C_{p-2}^q + C_{p-2}^{q-2}.$$

Exemple III. — Décomposer le tableau des combinaisons C_p^q par la considération de trois lettres a, b, c.

Combinaisons ne contenant aucune des trois lettres........	C_{p-3}^q
» contenant une des trois lettres..............	$C_3^1 C_{p-3}^{q-1}$
» » deux des trois lettres.............	$C_3^2 C_{p-3}^{q-2}$
» » les trois lettres..................	$C_3^3 C_{p-3}^{q-3}$.

On a donc la formule

$$C_p^q = C_{p-3}^q + 3C_{p-3}^{q-1} + 3C_{p-3}^{q-2} + C_{p-3}^{q-3}.$$

On trouve, par induction, la formule suivante

$$C_p^q = C_{p-r}^q + C_r^1 C_{p-r}^{q-1} + C_r^2 C_{p-r}^{q-2} + \ldots + C_r^r C_{p-r}^{q-r},$$

ou, sous la forme *symbolique*,

(1) $$C_p^q \triangleq C_{p-r}^{q-r}(C+1)^r,$$

en considérant les *indices supérieurs* comme des exposants. On peut démontrer directement cette formule par la considération de r lettres déterminées, ou la vérifier *a posteriori*. (*Voir* un de nos articles dans la *Nouvelle Correspondance mathématique*, t. II, p. 70.

Exemple IV. — Si l'on désigne par a_p le nombre des arrangements simples de a lettres prises p à p, on a la formule

$$(a+b)_p = a_p + \frac{p}{1} a_{p-1} b_1 + \frac{p(p-1)}{1.2} a_{p-2} b_2 + \ldots + b_p,$$

que l'on appelle formule du *binôme des factorielles* de VANDERMONDE.

En effet, $(a+b)_p$ est le nombre des arrangements simples de $(a+b)$ lettres prises p à p; si l'on partage ces lettres en deux groupes, l'un de a lettres, l'autre de b lettres, ces arrangements pourront se diviser en différentes classes

1° Arrangements ne contenant que des lettres du premier groupe;						
2°	»	contenant	$(p-1)$ lettres du premier groupe et	1	du second	;
3°	»	»	$(p-2)$ »	2	»	;
4°	»	»	$(p-3)$ »	3	»	;

....

Cherchons combien il y a d'arrangements de la $(q+1)^{\text{ième}}$ classe. Nous commençons par former les arrangements des a lettres du premier groupe prises $(p-q)$ à $(p-q)$; dans ces arrangements, on introduira q lettres du second groupe et l'on variera leur ordre de toutes les manières possibles, sans changer l'ordre des premières, ce qui peut se faire de p_q manières, et l'on obtiendra ainsi $p_q a_{p-q}$ arrangements distincts de $(a+b)$ lettres

prises q à q. Enfin, comme il y a $\frac{b_q}{q!}$ manières de prendre q lettres du second groupe, le nombre des arrangements distincts de la classe de rang $(q+1)$ est

$$\frac{p_q}{q!} a_{p-q} b_q \quad \text{ou} \quad C_p^q a_{p-q} b_q.$$

En faisant varier q de o à p et faisant la somme, on trouve la formule donnée.

Si l'on remplace les arrangements simples par les arrangements complets, on retrouve la formule du binôme (n° 40).

49. Combinaisons complètes. — Les *combinaisons complètes* (ou *avec répétition*) de p objets, pris q à q, sont les groupes que l'on peut former avec q de ces objets, ces objets pouvant être pris jusqu'à q fois, de telle sorte que deux groupes diffèrent par le choix et non par l'ordre des objets.

Si l'on désigne par D_p^q le nombre des combinaisons complètes, on a :

Nombre des lettres du Tableau D_p^q...........	$q\ D_p^q$
Nombre de fois que a se trouve dans D_p^q.......	$\frac{q}{p}\ D_p^q$
Nombre des combinaisons contenant a.........	D_p^{q-1}
Nombre de fois que a se trouve dans D_p^{q-1}	$\frac{q-1}{p} D_p^{q-1}$.

Par suite,

$$q\,D_p^q = (p+q-1)\,D_p^{q-1},$$

d'où l'on déduit

$$D_p^q = \frac{p(p+1)\dots(p+q-1)}{q!}.$$

Ainsi, *le nombre des combinaisons complètes de p objets, pris q à q, est le produit des q nombres entiers croissants à partir de p, divisé par le produit des q premiers nombres.*

En renversant l'ordre des facteurs du numérateur de D_p^q, on a

$$D_p^q = C_{p+q-1}^q;$$

ainsi, le *nombre des combinaisons complètes de p objets, pris q à q, est égal au nombre des combinaisons simples de $(p+q-1)$ objets, pris q à q.* On peut démontrer directement ce résultat de la manière suivante. Désignons par

$$d_1,\ d_2,\ d_3,\ \dots,\ d_p,$$

Exemple III. — Décomposer le tableau D_p^q par la considération de trois lettres a, b, c.

Combinaisons ne contenant aucune des trois lettres ...	D_{p-3}^q
» contenant une des trois lettres..........	$C_3^1 D_{p-2}^{q-1}$
» » deux des trois lettres.........	$C_3^2 D_{p-1}^{q-2}$
» » les trois lettres...............	$C_3^3 D_p^{q-3}$

On a donc la formule

$$D_p^q = D_{p-3}^q + 3D_{p-2}^{q-1} + 3D_{p-1}^{q-2} + D_p^{q-3}.$$

On trouve, par induction, la formule suivante

$$D_p^q = D_{p-r}^q + C_r^1 D_{p-r+1}^{q-1} + C_r^2 D_{p-r+2}^{q-2} + \ldots + D_p^{q-r}.$$

On peut démontrer directement cette formule par la considération de r lettres déterminées, ou la vérifier *a posteriori*.

Si l'on exprime les combinaisons complètes au moyen des combinaisons simples, on trouve une formule qui ne diffère pas sensiblement de la formule (1) du n° 48 (*Ex. III*).

51. Les inversions. — Il y a *inversion* ou *dérangement* dans une permutation de nombres, inégaux deux à deux, écrits sur une ligne horizontale, toutes les fois qu'un nombre se trouve placé à la gauche d'un nombre plus petit.

Pour compter le nombre des inversions, on peut procéder de deux manières différentes, soit en comptant pour chaque terme le nombre des termes qui sont à la droite plus petits que lui, soit en comptant pour chaque terme le nombre de ceux qui sont à la gauche plus grands que lui, et en faisant le total pour tous les termes dans l'un ou l'autre cas.

On divise les permutations de n nombres en deux classes, suivant que le nombre des inversions est pair ou impair. Les deux classes sont également nombreuses.

L'échange de deux éléments quelconques d'une permutation change la classe de la permutation. Plus généralement, un nombre pair d'échanges d'éléments quelconques d'une permutation n'en modifie pas la classe ; un nombre impair d'échanges produit sur la permutation primitive un changement de classe. (Bézout.)

Exemple I. — Déterminer le nombre total D_n des inversions dans le tableau des P_n permutations de n éléments. Écrivons d'abord $(n+1)$ fois

le tableau P_n, nous obtenons ainsi $(n+1)D_n$ dérangements. Plaçons maintenant le $(n+1)^{\text{ième}}$ élément à la dernière place, à l'avant-dernière, ..., à la seconde place, à la première dans chacun des tableaux; nous produisons successivement pour chaque permutation

$$0, \quad 1, \quad 2, \quad \ldots, \quad (n-1), \quad n$$

nouveaux dérangements et nous avons construit le tableau des P_{n+1} permutations de $(n+1)$ éléments. On a donc

$$D_{n+1} = (n+1) D_n + \frac{n(n+1)}{2} P_n.$$

Posons $D_n = P_n Q_n$, il vient

$$Q_{n+1} = Q_n + \frac{n}{2};$$

remplaçons successivement n par $1, 2, 3, \ldots, (n-1)$, et faisons la somme des égalités obtenues; nous trouvons

$$Q_n = \frac{n(n-1)}{4} \qquad \text{et} \qquad D_n = \tfrac{1}{2} P_n C_n^2.$$

On vérifie immédiatement ce résultat en observant que le nombre total des inversions d'une permutation et de la permutation renversée est égal au nombre C_n^2 des combinaisons de n éléments pris deux à deux.

Exemple II. — Le nombre total des inversions contenues dans les permutations circulaires de n éléments est $\frac{1}{6}(n-1)n(n+1)$.

52. Les cycles. — On peut encore déterminer la classe d'une permutation par la méthode plus expéditive des cycles, due à CAUCHY. Considérons une permutation quelconque de quinze nombres, et plaçons au-dessus de chacun de ses termes les nombres entiers suivant l'ordre ordinaire

$$\begin{array}{l} 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15; \\ 8,\ 6,\ 12,\ 1,\ 5,\ 14,\ 2,\ 11,\ 13,\ 15,\ 4,\ 9,\ 3,\ 10,\ 7. \end{array}$$

Au-dessous de 1 se trouve 8; au-dessous de 8 se trouve 11; au-dessous de 11 se trouve 4; au-dessous de 4 se trouve 1. On forme ainsi le premier cycle

$$1, 8, 11, 4.$$

En partant du nombre 2, on forme un deuxième cycle

$$2, 6, 14, 10, 15, 7.$$

En partant du nombre 3, qui ne figure pas dans les deux cycles précédents, on forme un troisième cycle

$$3,\ 12,\ 9,\ 13;$$

enfin il reste le cycle formé par un seul nombre, 5.

Cela posé, l'échange de deux éléments augmente ou diminue, de 1, le nombre des cycles de la permutation, suivant que les éléments échangés appartiennent au même cycle ou à des cycles différents. On en déduit que deux permutations appartiennent à une même classe ou à des classes différentes suivant que les nombres de leurs cycles sont ou ne sont pas de même parité.

Pour déterminer la classe, on remarquera que la permutation suivant l'ordre naturel contient un nombre de cycles égal au nombre des éléments de la permutation.

La théorie des inversions et des cycles trouve son application dans un grand nombre de questions d'Algèbre; le lecteur trouvera une interprétation intéressante de cette théorie dans le *jeu du Taquin* (voir nos *Récréations mathématiques*).

Exemple I. — On appelle *écart* d'un élément la différence entre son rang dans la suite naturelle et son rang dans une permutation. Démontrer que si l'on supprime un terme quelconque d'une permutation des n premiers entiers, la variation du nombre des inversions est de même parité que l'écart du terme.

Exemple II. — Après avoir formé le tableau C_p^q des combinaisons simples de p lettres, prises q à q, on suppose que α lettres deviennent les mêmes que a; quel est le nombre des combinaisons différentes?

Les combinaisons qui contiennent r fois a sont en nombre

$$C_{p-\alpha}^{q-r},$$

et il faut faire la somme de ces expressions de $r = 0$ à $r = \alpha$.

Exemple III. — On forme le tableau des arrangements simples A_p^q de p lettres prises q à q; on suppose ensuite que α lettres sont les mêmes que a; combien y a-t-il d'arrangements différents?

Les arrangements qui contiennent r fois a correspondent, en retirant cette lettre, à une combinaison $C_{p-\alpha}^{q-r}$; introduisons r fois a dans cette combinaison et permutons les lettres de toutes les manières possibles : nous obtenons des arrangements différents en nombre

$$\frac{q!}{r!}\,C_{p-\alpha}^{q-r},$$

et il faut ensuite faire la somme de ces expressions de $r = 0$ à $r = \alpha$, en supposant $0! = 1$.

Exemple IV. — Parmi toutes les permutations de q lettres, combien y en a-t-il qui contiennent une, deux, trois, ..., lettres à des rangs désignés.

Exemple V. — On a la formule

$$n C_p^n + (n-1) C_p^{n-1} C_q^1 + (n-2) C_p^{n-2} C_q^2 + \ldots = \frac{pn}{p+q} C_{p+q}^n.$$

En effet, soient p objets d'une première espèce et q d'une seconde. Si l'on forme toutes les combinaisons de ces $(p+q)$ objets, pris n à n, et que dans chacune d'elles on mette successivement à la première place chacun des objets qui s'y trouvent, sans s'occuper de l'ordre des autres, le nombre des dispositions obtenues sera $n C_{p+q}^n$.

Ces dispositions peuvent se partager en deux classes: celles qui commencent par un des p objets de la première espèce et celles qui commencent par un des q objets de la seconde espèce. Le nombre des groupes de la première classe est précisément le premier membre de la formule à démontrer, et, comme chacun des objets se trouve au premier rang le même nombre de fois, le rapport du nombre des dispositions de la première classe au nombre total des dispositions est égal à $\frac{p}{p+q}$. (H. LAURENT.)

CHAPITRE VII.

LA GÉOMÉTRIE DE SITUATION.

Nous placerons ici quelques considérations générales sur plusieurs problèmes de la Géométrie de situation; ces problèmes se rapportent directement à l'Arithmétique, car leur solution dépend de la théorie des combinaisons.

LES ÉCHIQUIERS ARITHMÉTIQUES.

Nous avons montré, au Chapitre VI, l'emploi de l'échiquier, pour la solution de divers problèmes d'Arithmétique; nous donnerons encore, dans ce Chapitre et dans les suivants, quelques autres exemples qui permettent de simplifier et de généraliser les méthodes de solution de problèmes célèbres, dont la difficulté avait été signalée par Euler; nous citerons, en particulier, le problème des rencontres et celui de la décomposition d'un polygone en triangles, par des diagonales.

Tout échiquier arithmétique est un tableau, fini ou indéfini, de nombres placés dans les cases de carrés égaux et contigus : ces termes se déduisent les uns des autres d'après une loi de formation spéciale, linéaire, permanente dans toute l'étendue du tableau; les conditions initiales peuvent être arbitraires; mais, en général, on suppose connus tous les termes d'une colonne verticale et ceux d'une demi-rangée horizontale ou diagonale. Ainsi, tout tableau de sommes et de différences est un échiquier arithmétique; d'ailleurs on a immédiatement cette propriété fondamentale : Si plusieurs échiquiers ont la même loi de formation, il en est de même pour l'échiquier obtenu en superposant les échiquiers donnés, après avoir multiplié tous les termes d'un même échiquier, par un nombre quelconque, positif ou négatif.

53. Le carré arithmétique. — Il est défini par une colonne et par une demi-rangée d'unités; on forme un terme quelconque par l'addition de celui qui le précède et de celui qui le surmonte.

Fig. 32.

F → y							
1	1	1	1	1	1	1	1
1	2	3	4	5	6	7	8
1	3	6	10	15	21	28	36
1	4	10	20	35	56	84	120
1	5	15	35	70	126	210	330
1	6	21	56	126	252	462	792
1	7	28	84	210	462	924	1716
1	8	36	120	330	792	1716	3432

x

Carré arithmétique de Fermat.

Si l'on désigne par F_x^y le terme contenu dans la $(x+1)^{\text{ième}}$ ligne et dans la $(y+1)^{\text{ième}}$ colonne, on a par définition

$$F_x^y = F_x^{y-1} + F_{x-1}^y.$$

On forme ainsi le triangle arithmétique de Pascal, dans une disposition spéciale plus symétrique et plus commode pour la suite des calculs; d'ailleurs la loi de formation nous montre que tout terme F_x^y du tableau est le nombre de manières de se rendre de la case (o, o) à la case (x, y), comme dans la marche de la tour au jeu des échecs, par déplacements d'un seul pas dans les deux sens ↓ et →. Si l'on désigne les deux sens par a et b, à chacun des déplacements indiqués correspond une permutation avec répétition de x lettres a et de y lettres b, et inversement. On a donc

$$F_x^y = C_{x+y}^x = \frac{(x+y)!}{x!\,y!} = C_{x+y}^y = F_y^x.$$

Le carré arithmétique ne diffère pas du Tableau des nombres figurés, qui a été étudié par Fermat (n° 38); mais la méthode de calcul pour obtenir l'expression d'un terme quelconque du Tableau, en ne passant que par les permutations avec répétition de deux éléments, est beaucoup plus simple que la méthode anté-

rieure de FERMAT, pour le calcul des nombres figurés et des combinaisons.

54. Échiquier triangulaire. — Il a été considéré par M. DELANNOY et appliqué à la solution de problèmes difficiles sur le Calcul des probabilités (¹). Dédoublons le carré arithmétique, changeons tous les signes du carré supérieur et transportons-le sur l'autre, de telle sorte que la parallèle au-dessous de la diagonale ↘ vienne coïncider avec la parallèle située au-dessus; nous obtenons alors une transversale formée de zéros, et en nous bornant à la partie commune des deux échiquiers qui est située au-dessous de cette ligne, nous avons le Tableau (*fig.* 33)

Fig. 33.

T → y ; ↓ x

1	0							
1	1	0						
1	2	2	0					
1	3	5	5	0				
1	4	9	14	14	0			
1	5	14	28	42	42	0		
1	6	20	48	90	132	132	0	
1	7	27	75	165	297	429	429	0

Échiquier triangulaire de Delannoy.

La loi de formation de l'échiquier est semblable à celle du carré arithmétique; chacun des termes du Tableau représente le nombre de manières de se rendre de la première case, par déplacements successifs d'un seul pas, dans les deux sens ↓ et →, mais sans traverser la diagonale, c'est-à-dire de telle sorte qu'à un instant quelconque le nombre des pas horizontaux ne dépasse jamais le nombre des pas verticaux.

En désignant par T_x^y le terme de la $(x+1)^{\text{ième}}$ ligne et de la $(y+1)^{\text{ième}}$ colonne, on a, par définition,

$$T_x^y = F_x^y - F_{x-1}^{y+1},$$

(¹) H. DELANNOY, *Emploi de l'échiquier pour la solution de problèmes arithmétiques*. Congrès de Nancy, Paris et Limoges. — *Sur la durée du jeu* (*Bulletin de la Société mathématique*, t. XVI).

et, par suite,

$$T_x^y = \frac{x-y+1}{x+1} C_{x+y}^y,$$

Pour les nombres de la diagonale,

$$T_x^x = \frac{1}{x+1} C_{2x}^x.$$

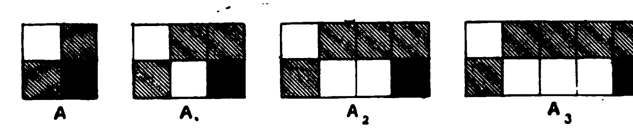
Si l'on continue le Tableau au-dessus de la ligne des zéros, on voit immédiatement que les termes symétriquement placés par rapport à cette ligne sont égaux et de signes contraires.

REMARQUE. — On voit encore que les termes du Tableau, renfermés dans l'angle xTy, et situés sur une même parallèle à la diagonale $\nearrow$, sont respectivement les coefficients du développement de

$$(1-z)(1+z)^n.$$

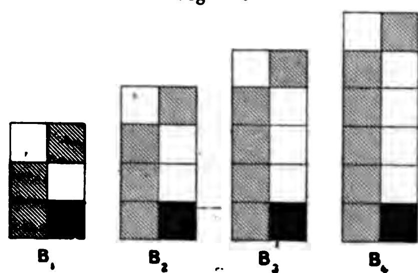
Le carré arithmétique possède de nombreuses propriétés qu'il est facile de déduire de celles que nous avons établies aux nos 4 et 10. On les trouve reproduites dans les *fig.* 34 et 35; par suite, les mêmes propriétés s'ap-

Fig. 34.



pliqueront à l'échiquier triangulaire supposé prolongé indéfiniment, en remplaçant T_x^y dans les formules, en fonction des combinaisons. On par-

Fig. 35.



vient ainsi à de nombreuses relations; on en obtient d'autres, en appliquant aux coefficients de $(1-z)(1+z)^n$ le procédé de démonstration

que nous avons indiqué au n° 74. Ainsi l'on peut trouver facilement, pour l'échiquier triangulaire restreint, la somme de termes consécutifs d'une ligne ou d'une colonne, la somme alternée de termes consécutifs d'une parallèle à la diagonale ascendante, ou la somme des carrés de tous les termes d'une telle ligne.

Exemple I. — Déterminer le nombre des permutations avec répétition de x lettres a et de y lettres b qui commencent par a ou par b.

On trouve respectivement

$$C_{x+y-1}^{y} \quad \text{et} \quad C_{x+y-1}^{y-1}.$$

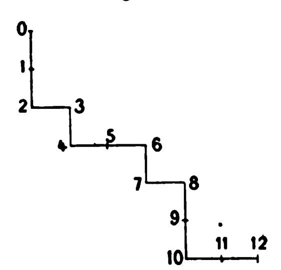
Exemple II. — Parmi les permutations qui commencent par a, déterminer le nombre de celles qui sont telles qu'en s'arrêtant à une lettre quelconque, le nombre des b ne soit jamais supérieur à celui des a.

On trouve $T_{x-1}^{y} = \dfrac{x-y}{x} C_{x+y-1}^{y}$; par suite, le nombre des permutations commençant par a, qui possèdent la propriété opposée, est $\dfrac{y}{x} C_{x+y-1}^{y}$.

Exemple III (*Problème des deux files de soldats*). — De combien de manières peut-on disposer des nombres tous différents sur deux rangées parallèles, de telle sorte que les nombres aillent toujours en croissant, de gauche à droite, et de haut en bas.

Supposons d'abord $n = 12$ et qu'il s'agisse de placer les nombres sur deux rangées égales, conformément aux conditions de l'énoncé. Considérons une des marches, par déplacements ↓ et → sur l'échiquier triangulaire de 6, pour se rendre de 0 sur le coin opposé en diagonale. Si l'on écrit

Fig. 36.



Les files de soldats.

successivement les nombres 1, 2, 3, ..., en passant de l'autre côté de la ligne, toutes les fois qu'elle se brise, et si l'on écrit sur deux rangs les nombres situés de part et d'autre, on forme le Tableau

$$\begin{array}{cccccc} 1, & 2, & 4, & 7, & 9, & 10, \\ 3, & 5, & 6, & 8, & 11, & 12, \end{array}$$

qui remplit les conditions de l'énoncé. Inversement, toute disposition sur deux rangées, conforme aux conditions de l'énoncé, conduit à une marche sur l'échiquier triangulaire. Ainsi, le nombre des files égales, pour $2n$ nombres donnés, a pour expression $T_n^n = \frac{1}{n+1} C_{2n}^n$.

Exemple IV. — Si l'on remplace T_n^n par t_n, on a la formule

$$t_{n+1} = t_0 t_n + t_1 t_{n-1} + \ldots + t_{n-1} t_1 + t_n t_0.$$

En effet, si l'on considère l'échiquier triangulaire ayant $a_0 a_{n+1}$ pour hypoténuse, t_{n+1} désigne le nombre des marches par pas $\downarrow$ et $\rightarrow$ pour aller de a_0 à a_{n+1}. Le nombre de celles qui passent par a_p, sans passer par $a_1, a_2, \ldots, a_{p-1}$, est évidemment égal au nombre des marches de b_1 à b_{n-p}, multiplié par le nombre des marches de a_{n-p} à a_{n+1}, c'est-à-dire à $t_{n-p} t_p$. En faisant $p = 1, 2, \ldots, n$, et en sommant, on obtient la formule demandée.

Fig. 37.

a_0	.	.	.	.	.
b_1	a_1	.	.	.	.
.	b_2	a_2	.	.	.
.	.	b_3	a_3	.	.
.	.	.	b_4	a_4	.
.	.	.	.	b_5	a_5

Exemple V. — Démontrer la formule

$$t_{n-1} - C_n^1 t_{n-2} + C_{n-1}^2 t_{n-3} - \ldots = 0.$$

Exemple VI. — Trouver la somme de tous les termes contenus dans les x premières lignes et les y premières colonnes du carré arithmétique.

Exemple VII. — Si l'on remplace, pour abréger, $F_n^n = C_{2n}^n$ par q_n, et si l'on suppose $q_0 = 1$, on a la formule

$$q_0 q_n + q_1 q_{n-1} + \ldots + q_{n-1} q_1 + q_n q_0 = 2^{2n}.$$

Cette formule se démontre, comme à l'*Exemple IV*, en classant les marches de la tour qui joignent l'origine à toutes les cases d'une parallèle à la diagonale ascendante $\nearrow$, d'après le nombre de celles qui vont de l'origine à a_n et qui passent par a_p, sans passer par $a_1, a_2, \ldots, a_{p-1}$ (*fig.* 37).

Exemple VIII. — Démontrer que la somme alternée

$$q_0 q_n - q_1 q_{n-1} + q_2 q_{n-2} - \ldots + (-1)^n q_n q_0$$

est nulle pour n impair, et égale à $2^n q_\nu$ pour n pair égal à 2ν.

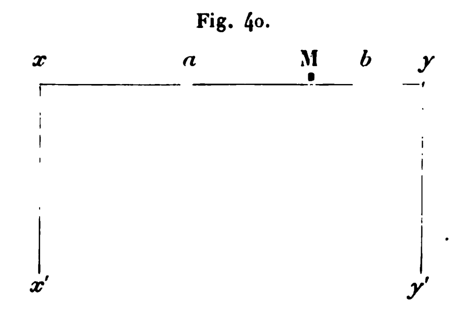
ou (2) représente le terme d'un échiquier pentagonal, soumis à la loi de formation du carré arithmétique. Et l'on sait qu'il en est de même dans la superposition d'échiquiers soumis à cette même loi. C. Q. F. D.

La considération de l'échiquier hexagonal de M. Delannoy permet de résoudre immédiatement le problème suivant sur le jeu de dames. Une solution beaucoup moins simple a été donnée dans un intéressant Mémoire, par M. D. André (*Bulletin de la Soc. math.*, t. VII, p. 43).

Exemple I. — Sur un damier présentant une largeur donnée de cases et une hauteur indéfinie, par combien de chemins un pion qui ne recule jamais et qui part d'une case donnée peut-il arriver à une autre case donnée?

Le déplacement du pion, au jeu de dames, se fait par pas successifs, dans les deux sens ↙↘, sur des cases de même couleur, tandis que les bords du damier xx' et yy' sont parallèles à la direction ↓. Soit M la position

Fig. 40.



du pion sur le bord supérieur du damier, de telle sorte que xM et My contiennent respectivement a et b cases. Si l'on fait tourner le damier d'un demi-quart de tour dans le sens opposé aux aiguilles d'une montre, les déplacements du pion deviennent parallèles aux directions ↓ et →, c'est-à-dire parallèles à ceux d'une tour, tandis que les bords verticaux xx' et yy' deviennent parallèles à la diagonale ↘. On est ainsi ramené à la considération de l'hexagone arithmétique. (*Voir* n° 6, *Exemple III.*)

LES POLYGONES.

57. Décomposition des polygones convexes. — Il s'agit de trouver toutes les manières de décomposer un polygone convexe en triangles au moyen de diagonales qui ne se rencontrent pas dans l'intérieur du polygone. On observera d'abord que *le nombre des diagonales d'un polygone convexe est égal à* $\frac{1}{2}n(n-3)$, puis-

mais on suppose à l'avance que les cases de deux transversales parallèles à la diagonale descendante ↘ sont garnies de zéros.

Fig. 39.

H — y ; x

1	1	1	1	0			
1	2	3	4	4	0		
1	3	6	10	14	14	0	
0	3	9	19	33	47	47	0
	0	9	28	61	108	155	155
		0	28	89	197	352	507

Hexagone arithmétique de Delannoy.

Ainsi la *fig.* 39 représente l'hexagone arithmétique pour $a = 3$ et $b = 4$, en désignant par a l'abscisse du zéro de la première colonne et par b l'ordonnée du zéro de la première ligne. Un terme quelconque H_x^y de l'hexagone est la somme de l'une ou l'autre des suites de différences

$$(1) \qquad (-1)^h\left[C_{x+y}^{x-h(a+b)} - C_{x+y}^{y-h(a+b)-b}\right],$$

ou

$$(2) \qquad (-1)^h\left[C_{x+y}^{y-h(a+b)} - C_{x+y}^{x-h(a+b)-b}\right],$$

pour toutes les valeurs o, 1, 2, 3, ..., h de h qui ne rendent pas négatifs les indices supérieurs. En effet, on voit d'abord que ces deux sommes sont les mêmes; car chacun des premiers termes d'une différence quelconque de la première suite est égal au dernier terme de la différence de rang précédent dans la seconde suite. On voit ensuite que, pour $x = y - b$, c'est-à-dire pour tous les nombres situés sur la parallèle supérieure à la diagonale, au-dessus, on a $H_x^y = 0$, car toutes les différences (1) s'annulent; de même, pour $y = x - a$, c'est-à-dire pour tous les nombres situés sur la parallèle au-dessous de la diagonale, on a encore $H_x^y = 0$, car toutes les différences (2) s'annulent. En outre, sur les axes Hx et Hy, pour $x = 0$ et $y < b$ ou pour $y = 0$ et $x < a$, chaque terme de l'une ou l'autre des expressions précédentes donne $H_x^y = 1$. D'ailleurs, toute différence donnée par l'une des expressions (1)

supprime le triangle AKL, il reste un polygone de $(x+2)$ côtés divisé en x triangles; mais, du sommet A, il ne part plus que $(x-y-1)$ diagonales, puisque AK devient un côté.

Dans le second cas, si une ou plusieurs diagonales aboutissent en L, la diagonale AK n'est pas tracée, et si l'on considère le faisceau des diagonales tracées du point L, on peut faire glisser son sommet le long de LK jusqu'en K; mais l'une des diagonales du faisceau vient coïncider, soit sur le côté KH, soit sur une autre diagonale tirée de K; on remplace alors la diagonale supprimée par AK, et l'on obtient ainsi une décomposition d'un polygone de $(x+3)$ côtés, mais avec une diagonale en plus aboutissant au sommet A. En faisant l'opération inverse, on démontre l'exactitude de la formule de récurrence et, par suite, celle de la formule précédente.

Ainsi, *le nombre des décompositions d'un polygone de* $(x+3)$ *côtés par* x *diagonales, et telles que* $(x-y)$ *diagonales aboutissent à un sommet désigné, est égal à*

$$(1) \qquad P_{x+3}^{x-y} = \frac{x-y+1}{x+1} C_{x+y}^{y}.$$

Pour obtenir *le total* P_{n+2} *de toutes les décompositions d'un polygone de* $(n+2)$ *côtés en triangles,* il suffit de prendre la somme de tous les termes de la ligne correspondante de l'échiquier triangulaire; mais cette somme est égale au nombre placé immédiatement au-dessous du dernier terme considéré. On a donc

$$(2) \qquad P_{n+2} = \frac{1}{n+1} C_{2n}^{n} = \frac{(2n)!}{n!(n+1)!} = 2^n \frac{1.3.5\ldots(2n-1)}{(n+1)!}.$$

Au lieu de tracer $(n-3)$ diagonales d'un polygone de n côtés, pour le décomposer, on peut en tracer une de moins, et la décomposition contient un quadrilatère. En suivant notre méthode, on peut construire le tableau des décompositions par la considération d'un sommet désigné. On peut aussi tracer deux diagonales de moins, et chaque décomposition contiendra deux quadrilatères ou un pentagone, et ainsi de suite. On arrive ainsi à de nombreuses formules que nous laissons au lecteur le soin d'établir. En prenant, dans chaque cas, le total des solutions pour un polygone de n côtés, on parvient à la démonstration de ce théo-

rème, énoncé par Prouhet sous une forme peu différente (*Nouv. Ann. de Math.*, 2[e] série, t. V, p. 384).

Le nombre X_n^d des manières de décomposer un polygone convexe de n côtés, en $(d+1)$ parties, au moyen de d diagonales qui ne se coupent pas à l'intérieur du polygone, est

$$X_n^d = \frac{1}{d+1} C_{n-3}^d D_n^d.$$

Les lettres C et D désignent respectivement des combinaisons simples et des combinaisons complètes. En remplaçant n par $(n+2)$ et d par $(n-1)$, on retrouve la formule (2). D'ailleurs, on peut encore étudier le cas où l'on trace, dans un polygone de n côtés, plus de $(n-3)$ diagonales, avec certaines conditions d'intersection.

Remarque. — En résumé, les problèmes suivants : *Décomposition d'un polygone en triangles. — Les deux files de soldats. — Permutations figurées qui coïncident avec elles-mêmes en faisant tourner l'échiquier d'un quart de tour. — Permutations figurées symétriques par rapport à une diagonale et n'ayant aucune tour sur cette diagonale. — Manières d'effectuer le produit de facteurs inégaux. — Déplacements de la tour sur l'échiquier triangulaire. — Permutations avec répétition de deux lettres. — Marches du pion au jeu de dames*, et d'autres, que nous traiterons plus tard, tels que *Les fractions étagées. — Le scrutin de ballottage*, reviennent l'un à l'autre, tant il est vrai que les vérités mathématiques de l'ordre arithmétique sont peu nombreuses; souvent des vérités qui paraissent distinctes et éloignées l'une de l'autre ne diffèrent que par la forme extérieure et, en quelque sorte, par le vêtement qui les couvre.

Exemple I. — Le nombre des points d'intersection des diagonales d'un polygone de n côtés, à l'intérieur de ce polygone, est égal à C_n^4, si trois diagonales ne concourent pas en un même point. — En effet, le nombre de ces points est égal au nombre C_n^4 des quadrilatères intérieurs que l'on peut former avec quatre des n sommets du polygone.

Exemple II. — Si l'on joint de toutes les manières possibles n points d'un plan, les lignes de jonction se coupent en $3C_n^4$ nouveaux points.

En effet, les côtés opposés des quadrilatères considérés dans l'exemple

précédent se coupent en deux autres points, distincts des sommets et du point d'intersection des diagonales.

Autrement. — Le nombre de toutes les lignes de jonction est C_n^2; le nombre de toutes les lignes de jonction qui ne passent pas par deux points désignés est C_{n-2}^2; par suite, puisque chaque point d'intersection se trouve sur deux droites, le nombre des points d'intersection de toutes les lignes, autres que les n points donnés, est

$$\tfrac{1}{2} C_n^2 C_{n-2}^2 = \frac{n(n-1)(n-2)(n-3)}{8} = 3C_n^4.$$

Exemple III. — Dans un polygone convexe de n côtés, le nombre des points extérieurs d'intersection des diagonales est égal à

$$\tfrac{1}{12} n(n-3)(n-4)(n-5).$$

En effet, le nombre des diagonales qui ne passent pas par deux sommets désignés est

$$\tfrac{1}{2} n(n-3) - 2(n-3) + 1 = \tfrac{1}{2}(n^2 - 7n + 14);$$

par suite, le nombre de tous les points d'intersection des diagonales, tant à l'intérieur qu'à l'extérieur du polygone, est

$$\tfrac{1}{8} n(n-3)(n^2 - 7n + 14);$$

si l'on en retranche le nombre C_n^4 des points d'intersection à l'intérieur du polygone, on trouve la formule demandée.

Exemple IV. — Ancienne méthode pour trouver le nombre des manières de décomposer un polygone en triangles par des diagonales.

Soit ABC...HKL un polygone de $(n+1)$ côtés; désignons par P_{n+1} le nombre des manières de le décomposer en triangles. Le nombre des décompositions dont fait partie le triangle ABC est évidemment P_n, nombre de décompositions du polygone AC...HKL; le nombre des décompositions dont fait partie le triangle ABD est $P_3 P_{n-1}$, car le triangle BCD peut se combiner avec chacun des P_{n-1} modes de décomposition relatifs au polygone ADE...KL; le nombre des décompositions dont fait partie le triangle ABE est $P_4 P_{n-2}$, car chaque mode relatif au quadrilatère BCDE doit se combiner avec chacune des décompositions du polygone AEF...KL; et ainsi de suite. Puisque l'on obtient toutes les décompositions possibles et chacune une seule fois, on a donc

$$(1) \qquad P_{n+1} = P_n + P_3 P_{n-1} + P_4 P_{n-2} + \ldots + P_{n-1} P_3 + P_n.$$

Considérons maintenant le polygone ABC...HK de n côtés, et examinons les modes de décomposition dans lesquels on emploie chacune des diagonales issues du sommet A. Par un raisonnement analogue à celui qui

précède, on voit que pour AC le nombre des décompositions est $P_3 P_{n-1}$; pour AD il est égal à $P_4 P_{n-2}$, et ainsi de suite. En répétant la même opération pour tous les sommets, le nombre total des modes considérés sera donc

$$n(P_3 P_{n-1} + P_4 P_{n-2} + \ldots + P_{n-2} P_4 + P_{n-1} P_3).$$

On obtient de cette manière toutes les décompositions possibles; mais on les trouve ainsi plusieurs fois. En effet, chaque décomposition se fait au moyen de $(n-2)$ triangles ayant $(3n-6)$ côtés et dans lesquels les n côtés du polygone entrent chacun une seule fois; donc $(2n-6)$ côtés sont formés par les diagonales, et, comme chacune de celles-ci appartient à deux triangles, on voit que chaque mode emploie $(n-3)$ diagonales. Or toute décomposition doit évidemment se reproduire autant de fois que les $(n-3)$ diagonales qui y entrent ont d'extrémités, c'est-à-dire $(2n-6)$ fois; on a donc

$$P_n = \frac{n(P_3 P_{n-1} + P_4 P_{n-2} + \ldots + P_{n-2} P_4 + P_{n-1} P_3)}{2n-6}.$$

La comparaison des deux égalités précédentes donne

$$(2) \qquad P_{n+1} = \frac{4n-6}{n} P_n;$$

par suite

$$(3) \qquad P_{n+2} = \frac{2.6.10\ldots(4n-2)}{(n+1)!} = 2^n \frac{1.3.5\ldots(2n-1)}{(n+1)!}.$$

Ce problème célèbre a été posé par EULER à SEGNER, qui a donné la formule (1) dans le tome VII des *Novi Commentarii;* la formule (2) paraît due à EULER. Cette question a été développée par LAMÉ, CATALAN, RODRIGUES et BINET dans les tomes III et IV du *Journal de Liouville.* On a encore la formule

$$P_{n+1} - C_n^1 P_n + C_{n-1}^2 P_{n-1} - \ldots = 0.$$

Exemple V. — Connaissant le nombre t_1 des triangles ne contenant qu'une seule diagonale, dans la décomposition d'un polygone de n côtés en $(n-2)$ triangles par $(n-3)$ diagonales, trouver les nombres t_2 et t_3 des triangles contenant deux et trois diagonales.

On a immédiatement

$$t_1 + t_2 + t_3 = n - 2,$$
$$2t_1 + t_2 = n;$$

d'où l'on tire

$$t_2 = n - 2t_1,$$
$$t_3 = t_1 - 2.$$

Ainsi t_1 est au moins égal à 2. On peut former un tableau à double

entrée contenant les nombres des décompositions de P_n, en prenant pour coordonnées n et t_1; on obtiendra ainsi de nouvelles formules.

Exemple VI. — Le nombre des manières de décomposer un polygone de $(p-2)q+2$ côtés, en q polygones de p côtés, est

$$\frac{(pq-q)(pq-q-1)\ldots(pq-2q+2)}{1.2.3\ldots q}. \qquad \text{(H.-M. TAYLOR.)}$$

LES RÉSEAUX.

58. Les réseaux. — Un réseau géométrique est le système formé par des points A, B, C, ..., disposés d'une manière quelconque dans l'espace, et reliés entre eux par une ou plusieurs lignes, droites ou courbes, que l'on appelle *chemins*. Les points A, B, C, ... sont appelés *carrefours*. Un carrefour est dit *pair* ou *impair,* suivant que le nombre des chemins qui y aboutissent est pair ou impair. Un réseau est continu quand un mobile placé sur l'un des chemins, ou sur l'un des carrefours, peut se rendre à un autre point quelconque sans quitter les chemins. Dans son Mémoire sur le *Problème des ponts de Königsberg* (¹), EULER a indiqué deux théorèmes qui se rapportent à ce sujet. Nous donnerons d'abord l'énoncé et une démonstration très simple du premier d'entre eux.

Lorsqu'un réseau renferme des carrefours impairs, ceux-ci sont en nombre pair. — En effet, si l'on fait le compte de tous les chemins qui aboutissent à chacun des carrefours, la somme de tous les nombres obtenus est un nombre pair, puisque chaque chemin a été compté deux fois. Cette somme étant un nombre pair, il faut nécessairement que, parmi les nombres entiers qui l'ont fournie, ceux qui sont impairs soient en nombre pair.

Exemple I. — Calculer le nombre des *sauts du cavalier des échecs* sur un échiquier rectangulaire formé de p lignes et de q colonnes.

On peut passer de l'une des $(q-1)$ premières colonnes à la colonne sui-

---

(¹) EULER, *Solutio problematis ad Geometriam situs pertinentis,* dans les Mémoires de l'Académie des Sciences de Berlin, pour 1759. Pour plus de détails, voir nos *Récréations mathématiques,* t. I, au Chapitre intitulé : *Le jeu des ponts et des îles,* et une Note de M. EM. LEMOINE sur *Quelques questions de Géométrie de position* (Congrès d'Alger).

vante par $(p-2)$ sauts descendants et par le même nombre de sauts ascendants ; on a donc

$$2(p-2)(q-1)$$

sauts, et un nombre égal en chevauchant de la droite vers la gauche.

De même, en passant à la ligne précédente ou à la suivante, il y a un nombre de sauts égal au double de

$$2(p-1)(q-2).$$

Donc *le nombre des sauts du cavalier sur l'échiquier rectangulaire de pq cases, en comptant l'aller et le retour, est égal au double de*

$$(2p-3)(2q-3)-1.$$

Plus généralement, si le saut du cavalier se compose de r pas dans un sens et de s pas dans l'autre, en supposant r et s respectivement plus petits que p et q, le nombre des sauts du cavalier, en comptant l'aller et le retour, est le double de l'expression

$$(2p-r-s)(2q-r-s)-(r-s)^2;$$

cependant, on doit diviser ce nombre par 2, lorsque l'un des nombres r, s ou $(r-s)$ est nul.

On calcule le *nombre des pas du roi* en considérant celui-ci comme l'ensemble de deux cavaliers dont l'un des pas est 1 et l'autre 0 ou 1. On trouve ainsi le double de

$$4pq-3p-3q+2.$$

Sur l'échiquier de p^2 cases, la *tour* peut être considérée comme l'ensemble de cavaliers dont l'un des pas est nul, et dont l'autre est l'un quelconque des entiers plus petits que p. On trouve ainsi que le nombre des déplacements de la tour sur l'échiquier de p^2 cases est le double de

$$p^2(p-1).$$

Sur l'échiquier de p^2 cases, le système des *deux fous* peut être considéré comme l'ensemble de cavaliers dont les pas égaux sont tous les nombres entiers plus petits que p. On trouve ainsi que le nombre des déplacements des deux fous sur l'échiquier de p^2 cases est le double de

$$\tfrac{1}{3}p(p-1)(2p-1).$$

Enfin, la *reine* peut être considérée, dans son mouvement, comme l'ensemble d'une tour et des deux fous ; par suite, le nombre de ses déplacements est le double de

$$\tfrac{1}{3}p(p-1)(5p-1).$$

Exemple II. — Le nombre des manières de placer *deux reines* sur l'échiquier de p^2 cases, de telle sorte qu'elles ne soient pas en prise, c'est-à-dire qu'elles ne soient pas situées sur une même ligne parallèle aux bords ou aux diagonales de l'échiquier est

$$\tfrac{1}{6}p(p-1)(p-2)(3p-1).$$

En effet, ce nombre est égal à l'excès du nombre des combinaisons des p^2 cases, prises deux à deux, sur la moitié du nombre des déplacements possibles de la reine, ou

$$\frac{p^2(p^2-1)}{2}-\frac{p(p-1)(5p-1)}{3}.$$

Le même calcul s'applique à d'autres pièces de l'échiquier, et l'on trouve pour *deux rois*

$$(p-1)(p-2)(p^2+3p-2),$$

et pour *deux cavaliers*

$$\tfrac{1}{2}(p-1)(p^3+p^2-8p+16).$$

Exemple III. — *Le problème des tours au jeu des échecs.* — Soit un échiquier rectangulaire de dimensions p et q; le problème des r tours consiste à placer r tours sur les pq cases de l'échiquier, mais de telle sorte que deux quelconques d'entre elles ne soient pas situées sur une même ligne ou sur une même colonne. Désignons par E_r et E_{r-1} le nombre des solutions du problème des r tours et des $(r-1)$ tours sur cet échiquier; on a d'abord $E_1=pq$, et, en supposant $q \lesseqgtr p$, on voit que E_r est nul pour $r>q$. Si l'on supprime l'une des r tours d'une solution E_r, on obtient une solution E_{r-1}; mais, inversement, si l'on part d'une solution E_{r-1}, on peut placer la $r^{\text{ième}}$ tour sur l'une des

$$(p-r+1)(q-r+1)$$

cases libres; on a donc la formule

$$(1) \qquad rE_r=(p-r+1)(q-r+1)\,E_{r-1};$$

par suite, le nombre E_r est égal à l'une des quatre expressions équivalentes

$$(2) \qquad \frac{1}{r!}A_p^r A_q^r, \quad A_p^r C_q^r, \quad A_q^r C_p^r, \quad r!\,C_p^r C_q^r,$$

dans lesquelles les lettres A et C désignent respectivement des arrangements et des combinaisons simples.

Supposons qu'on ait groupé les cases de l'échiquier en deux portions absolument quelconques, continues ou discontinues, et que l'on connaisse

les solutions du problème des r tours sur l'un des échiquiers partiels, pour toutes les valeurs de $r = 0$ à $r = q$; nous allons montrer comment on peut obtenir les solutions des r tours sur l'autre échiquier partiel. Les solutions du problème des r tours sur l'échiquier de pq cases peuvent être distribuées en $(r+1)$ classes, de telle sorte que la classe de rang $(s+1)$ renferme les solutions contenant $(r-s)$ tours sur le premier échiquier partiel et s tours sur le second. Nous désignerons par T_r^s le nombre des solutions de cette classe; on a donc

$$(3) \qquad E_r = T_r^0 + T_r^1 + T_r^2 + \ldots + T_r^r.$$

Partons d'une solution de la classe s; il y aura $(p-r)$ colonnes et $(q-r)$ lignes formant $(p-r)(q-r)$ cases libres sur l'une desquelles on pourra poser une nouvelle tour; on obtiendra ainsi

$$(p-r)(q-r)T_r^{s-1}$$

positions qui appartiendront aux solutions du problème des $(r+1)$ tours sur l'échiquier de pq cases, et respectivement à la classe de rang s ou de rang $(s+1)$, selon que la tour aura été ajoutée sur le premier échiquier partiel ou sur le second. Mais, inversement, en partant d'une solution du problème des $(r+1)$ tours sur l'échiquier complet, on voit, par la suppression de l'une quelconque d'entre elles, que les solutions de la classe s ont été comptées $(r-s+2)$ fois chacune, et que celles de la classe $(s+1)$ ont été comptées s fois; on a donc

$$(4) \qquad (p-r)(q-r)T_r^{s-1} = (r-s+2)T_{r+1}^{s-1} + s\,T_{r+1}^{s}.$$

Les formules (3) et (4) permettent de résoudre le problème des $(r+1)$ tours sur le second échiquier partiel, lorsque le problème des r tours est connu sur chacun d'eux, c'est-à-dire lorsque l'on connaît les nombres

$$T_1^0,\ T_2^0,\ \ldots,\ T_r^0, \quad \text{et} \quad T_r^1,\ T_r^2,\ \ldots,\ T_r^r.$$

Soit, par exemple, l'échiquier carré de seize cases divisé en deux fragments; le premier échiquier partiel est formé des cases du coin, repré-

Fig. 41.

. × × .
× × × ×
× × × ×
. × × .

Échiquier de 16 cases.

sentées par des points (*fig.* 41); le second est représenté par des croix. On a, pour le premier échiquier partiel,

$$T_1^0 = 4, \qquad T_2^0 = 2, \qquad T_3^0 = 0, \qquad T_4^0 = 0;$$

la formule (4) devient

$$(4-r)^2 T_r^{s-1} = (r-s+2)\, T_{r+1}^{s-1} + s\, T_{r+1}^{s};$$

si l'on fait successivement

$r=1$,	$r=2$,	$r=3$,
$s=1, 2$,	$s=1, 2, 3$,	$s=1, 2, 3, 4$,

on trouve

$T_1^1 = 12$,	$T_2^1 = 32$,	$T_3^1 = 8$,	$T_4^1 = 0$,
	$T_2^2 = 38$,	$T_3^2 = 56$,	$T_4^2 = 4$,
		$T_3^3 = 32$,	$T_4^3 = 16$,
			$T_4^4 = 4$.

Considérons maintenant l'échiquier carré de 36 cases : le premier échi-

Fig. 42.

```
.  .  .  .  .  .
.  .  ×  ×  .  .
.  ×  ×  ×  ×  .
.  ×  ×  ×  ×  .
.  .  ×  ×  .  .
.  .  .  .  .  .
```

Échiquier de 36 cases.

quier partiel représenté par des croix est le second échiquier de la figure précédente; on a donc

$$T_1^0 = 12, \qquad T_2^0 = 38, \qquad T_3^0 = 32, \qquad T_4^0 = 4.$$

La formule de récurrence devient

$$(6-r)^2 T_r^{s-1} = (r-s+2)\, T_{r+1}^{s-1} + s\, T_{r+1}^{s},$$

et, si l'on fait successivement

$r=1$,	$r=2$,	$r=3$,	$r=4$,	$r=5$,
$s=1, 2$,	$s=1, 2, 3$,	$s=1, 2, 3, 4$,	$s=1, 2, 3, 4, 5$,	$s=1, 2, 3, 4, 5, 6$,

on trouve

$T_1^1 = 24$,	$T_2^1 = 224$,	$T_3^1 = 512$,	$T_4^1 = 272$,	$T_5^1 = 16$,	$T_6^1 = 0$,
	$T_2^2 = 188$,	$T_3^2 = 1280$,	$T_4^2 = 1896$,	$T_5^2 = 512$,	$T_6^2 = 8$,
		$T_3^3 = 576$,	$T_4^3 = 2576$,	$T_5^3 = 2016$,	$T_6^3 = 160$,
			$T_4^4 = 652$,	$T_5^4 = 1568$,	$T_6^4 = 384$,
				$T_5^5 = 208$,	$T_6^5 = 160$,
					$T_6^6 = 8$.

Considérons encore l'échiquier rectangulaire de 56 cases; le premier échiquier partiel contenant les points est équivalent au second échiquier partiel de la figure précédente; on a donc

$$T_1^0 = 24,\quad T_2^0 = 188,\quad T_3^0 = 576,\quad T_4^0 = 652,\quad T_5^0 = 208,\quad T_6^0 = 8,\quad T_7^0 = 0.$$

Fig. 43.

.	.	.	×	×	.	.	.
.	.	×	×	×	×	.	.
.	×	×	×	×	×	×	.
×	×	×	×	×	×	×	×
.	×	×	×	×	×	×	.
.	.	×	×	×	×	.	.
.	.	.	×	×	.	.	.

Échiquier de 56 cases.

On formera le Tableau (*fig.* 43)

32	632	3912	8912	6784	1200	16
	356	5568	25752	39904	17352	1152
		1704	19952	63104	56672	9648
			3532	28304	52152	18688
				2816	13104	9648
					632	1152
						16

Exemple IV. — Le problème des fous au jeu des échecs. — Il s'agit de placer des fous sur les 64 cases de l'échiquier, de telle sorte que deux quelconques d'entre eux ne soient pas en prise, c'est-à-dire ne soient pas situés sur l'une ou l'autre des diagonales ou sur leurs parallèles. Il est évident que les centres des cases blanches de l'échiquier peuvent être considérés comme placés sur les croix de la figure précédente, et la marche du fou devient celle de la tour. Donc, d'après le dernier calcul, on peut placer sur les cases blanches de l'échiquier

1, 2, 3, 4, 5, 6, 7

fous et les nombres des solutions correspondantes sont

32, 356, 1704, 3532, 2816, 632, 16.

Nous désignerons respectivement ces nombres par f_r, en prenant pour r l'une des valeurs de 1 à 7; d'ailleurs f_r est nul pour $r > 7$.

Sur les cases blanches et noires de l'échiquier, on pourra placer jusqu'à 14 fous, et si n désigne l'un des nombres entiers de 1 à 14, le nombre F_n de manières de placer n fous sur les 64 cases de l'échiquier est donné par

$$F_n = f_n + f_1 f_{n-1} + f_2 f_{n-2} + \ldots + f_{n-1} f_1 + f_n.$$

Pour $n = 8$, on trouve 22522960 solutions. (PEROTT, *Bulletin de la Soc. math.*, t. XI.)

Exemple V. — Le problème des reines. — Ce problème est traité complètement jusqu'aux échiquiers de 11 cases de côté, dans nos *Récréations mathématiques* (t. I, 2e édition).

59. **Le tracé des réseaux.** — Dans le Mémoire que nous avons cité plus haut, EULER a encore démontré la proposition suivante : *Tout réseau continu qui ne contient que des carrefours pairs peut être décrit d'un seul trait formant un circuit fermé, sans omission ni répétition, quel que soit le point de départ qui coïncide avec le point d'arrivée.*

Nous démontrerons ce théorème en même temps que le suivant, énoncé par CLAUSEN dans le n° 494 des *Astronomische Nachrichten : Tout réseau continu ayant 2 n points impairs peut être décrit en n traits continus, sans omission ni répétition, et non en un moindre nombre.*

En effet, si l'on part d'un point impair A et si l'on chemine au hasard, sans repasser sur la même voie, on sera forcé de s'arrêter à un certain endroit. En observant que, dans cette marche, on ne change point la parité des carrefours que l'on traverse, on en conclut que le point d'arrêt est un point impair B. En supprimant le parcours AB, on obtient un réseau qui ne contient plus que $(2n - 2)$ carrefours impairs. Après n parcours analogues, il ne peut donc rester qu'un ou plusieurs réseaux restreints dont les carrefours sont tous pairs.

Maintenant, si l'on part d'un point quelconque M d'un réseau restreint et si l'on chemine au hasard, sur de nouveaux chemins, on ne se trouvera arrêté qu'en revenant au point de départ après avoir décrit un circuit fermé. Lorsque l'on aura tracé un certain nombre de ces boucles, on aura parcouru tout le réseau ; mais, puisque celui-ci est continu, ces boucles peuvent se souder les unes sur les autres et sur les n chemins qui ont été décrits primitivement. Par suite, le réseau peut être décrit en n traits continus, et ne peut l'être en un moindre nombre. C. Q. F. D.

On a encore le curieux théorème suivant dû à TRÉMAUX, ancien élève de l'École Polytechnique : *Tout réseau continu peut être décrit d'un seul trait, en passant deux fois sur tous les chemins, sans qu'il soit nécessaire de connaître le plan du réseau.*

Pour obtenir la solution de cette question qui démontre qu'un labyrinthe n'est jamais inextricable, on applique les trois règles suivantes, en ayant le soin de tracer sur chaque chemin parcouru un petit trait transversal à l'entrée et à la sortie des carrefours.

1° En partant d'un carrefour initial quelconque, on suit une voie quelconque jusqu'à ce que l'on arrive à un chemin fermé ou à un nouveau carrefour. Si le chemin qu'on a suivi se trouve fermé, on revient sur ses pas et l'on peut alors considérer ce chemin comme supprimé, puisqu'il a été parcouru deux fois. Si le chemin aboutit à un carrefour, on prend une voie quelconque, au hasard, en ayant soin de marquer d'un trait transversal la voie d'arrivée et la voie de départ. On continue l'application de cette première règle, chaque fois que l'on arrive à un carrefour inexploré. Au bout d'un certain temps, on arrivera nécessairement à un carrefour déjà visité ; mais cette situation peut se présenter de deux manières différentes, selon que le chemin d'arrivée a déjà été suivi une première fois, ou ne contient encore aucune trace de passage.

2° En arrivant à un carrefour déjà visité, par une voie nouvelle, on doit rétrograder en marquant par deux traits, sur cette voie, l'arrivée au carrefour et le départ.

3° Lorsque l'on arrive à un carrefour déjà exploré par une voie déjà parcourue, on prend, avant tout, une voie nouvelle s'il en existe ou, à son défaut, une voie qui n'aura été parcourue qu'une seule fois.

Nous laisserons de côté la démonstration de ce théorème, que l'on trouve dans nos *Récréations mathématiques*, au Chapitre sur le *Jeu des labyrinthes*.

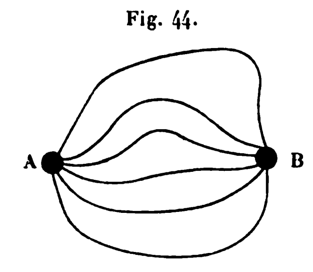
60. **Nombre des tracés des réseaux.** — Si l'on prend pour point de départ un point quelconque d'un réseau à carrefours pairs, on peut partir de ce point, dans deux sens différents, pour revenir au point initial. Par conséquent, le nombre des circuits complets est toujours un nombre pair, et le nombre des circuits est le même quel que soit le point de départ.

Considérons, par exemple, deux carrefours A et B réunis par $2n$ chemins qui ne s'entrecroisent pas ; le nombre des circuits distincts est égal à

$$2.1.2.3\ldots(2n-1), \quad \text{ou} \quad 2(2n-1)!$$

En effet, si l'on part d'un point quelconque, autre que A ou B, on a deux sens. En arrivant à l'un des carrefours, on a le choix entre $(2n-1)$ chemins ; puis, en arrivant à l'autre carrefour, entre $(2n-2)$ chemins, et ainsi de suite. On doit observer que, si l'on part d'un carrefour, le nombre des circuits semble être $(2n)!$ c'est-à-dire n fois le résultat précédent ; mais ces parcours ne sont

Fig. 44.



Réseau à deux carrefours.

pas distincts comme circuits. Il y a une différence de même nature dans les nombres de permutations d'objets disposés en ligne droite ou sur un circuit fermé (n° **34**). Afin d'éviter toute confusion, on évalue le nombre des circuits d'un réseau en partant d'un point et non d'un carrefour.

On ramène la recherche du nombre des tracés complets des réseaux à points impairs à la détermination du nombre des circuits des réseaux à carrefours pairs, par le théorème suivant : *Pour décrire, sans omission, ni répétition, un réseau ayant* $2n$ *carrefours impairs, en* n *traits et* n *sauts, pour revenir au point de départ, on joint ces points par* n *chemins de toutes les manières possibles, en nombre égal à*

$$N = 1.3.5\ldots(2n-3)(2n-1) = \frac{(2n)!}{2^n.n!},$$

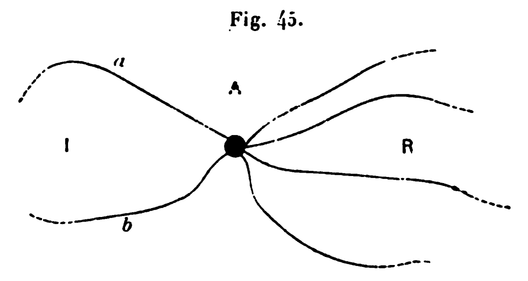
et le nombre cherché est la somme des nombres des circuits

des N *réseaux à carrefours pairs que l'on a obtenus*. On observera, d'ailleurs, que l'on ne doit sauter que d'un carrefour impair à un autre impair, et que le nombre des tracés est indépendant de la position du point de départ.

61. Théorèmes des impasses. — On appelle *impasse* tout fragment d'un réseau qui n'a d'autres points communs avec le reste du réseau que les extrémités de deux chemins, de telle sorte que la suppression d'une partie de chaque chemin détermine la séparation du réseau en deux autres; le réseau total se compose d'une impasse et d'un réseau partiel. Deux cas peuvent se présenter, suivant que les deux chemins de l'impasse aboutissent à un même point du réseau partiel ou à deux points différents.

Premier cas. — Supposons que les deux chemins a et b de l'impasse aboutissent à un carrefour A du réseau partiel; désignons par I et par R les nombres des circuits de l'impasse et du réseau partiel, et par $2p$ le nombre des chemins du réseau partiel qui

Fig. 45.



L'impasse à un seul carrefour.

aboutissent au carrefour A. Dans un circuit quelconque du réseau partiel, on passe p fois au carrefour A et, à l'un quelconque des passages, il faut décrire complètement un des circuits de l'impasse; par suite, le nombre des circuits du réseau total est

$$pIR.$$

Si le point A était un point simple du réseau partiel, on ferait $p = 2$. Si l'impasse était formée d'un seul chemin dont les extrémités viendraient aboutir au carrefour A, on ferait $I = 2$. Enfin, si q impasses indépendantes les unes des autres aboutissent au

carrefour A et si l'on désigne par I_1, I_2, ..., I_q les nombres de leurs circuits, on trouve, par la suppression successive des impasses, que le nombre des circuits du réseau total est

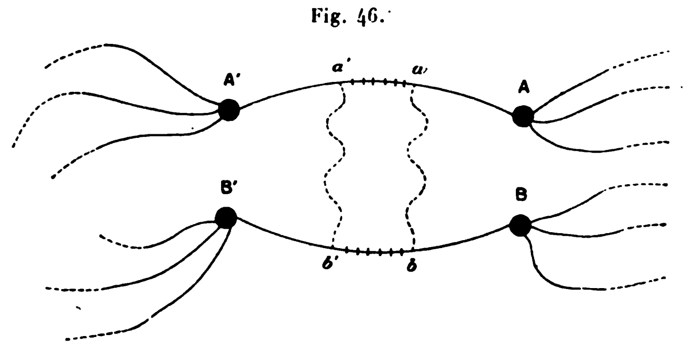
$$p(p+1)\ldots(p+q-1)\, I_1 I_2 I_3 \ldots I_q R.$$

Exemple I. — Le nombre des circuits formés par n circonférences égales, tangentes deux à deux, dont les centres sont en ligne droite, est 2^n.

Exemple II. — Le nombre des circuits d'une rosace à n feuilles est égal à $2^n(n-1)!$

Deuxième cas. — Supposons que les deux chemins a et b de l'impasse I aboutissent à deux carrefours A et B du réseau partiel R; alors ces carrefours sont impairs, ainsi que les premiers carrefours A′ et B′ de l'impasse, qui se trouvent sur les deux che-

Fig. 46.



L'impasse à deux carrefours.

mins. Pour évaluer le nombre des circuits du réseau total, partons du point a de AA′, dans un sens ou dans l'autre; il faut décrire l'impasse et le réseau partiel d'un seul trait, et dans un sens déterminé; par conséquent, le nombre total des circuits est

$$2\frac{I}{2}\frac{R}{2} \quad \text{ou} \quad \frac{IR}{2};$$

en d'autres termes, le nombre des circuits du réseau total est la moitié du produit des nombres de circuits de l'impasse et du réseau partiel. D'ailleurs, on observera que l'application de ce théorème est illusoire, si l'impasse I se réduit à une impasse simple.

Exemple III. — Les sommets A et B d'un rectangle ABCD sont réunis par $(2p-1)$ chemins; les sommets C et D par $(2q-1)$ chemins, les sommets A, D et les sommets B, C sont réunis par un seul chemin; calculer le nombre des circuits du réseau. — On trouve

$$2(2p-1)!\,(2q-1)!$$

62. Théorème des carrefours. — Pour évaluer le nombre des circuits d'un réseau à carrefours tous pairs, on commence par supprimer toutes les impasses qui peuvent exister. On ramène ensuite le réseau à un ou plusieurs autres contenant un carrefour en moins, et ainsi de suite, jusqu'à ce que les réseaux obtenus ne contiennent plus que deux carrefours. La suppression d'un carrefour se fait par l'emploi du théorème de M. G. Tarry [1] : *Lorsque $2n$ chemins $a, b, c, d, \ldots$, aboutissent à un carrefour, le nombre des circuits du réseau est égal à la somme des nombres des circuits des* N *réseaux obtenus en soudant deux par deux, de toutes les manières possibles, les n chemins $a, b, c, d, \ldots$; et d'ailleurs,*

$$N = 1.3.5\ldots(2n-1) = \frac{(2n)!}{2^n.n!}.$$

Dans l'application de ce théorème on doit faire les deux remarques suivantes : 1° Si la suppression d'un carrefour amène la désagrégation du réseau, on recommence l'opération après avoir appliqué les théorèmes des impasses. 2° Les N réseaux partiels obtenus par la suppression d'un carrefour ne sont pas toujours distincts, car deux réseaux sont équivalents lorsqu'ils possèdent le même nombre de carrefours et que deux carrefours quelconques sont réunis par le même nombre de chemins.

Exemple I. — Le nombre des circuits de la figure formée par les côtés et les diagonales d'un pentagone régulier, sans fragmenter les diagonales, est **264**.

Exemple II. — Le nombre des circuits formés par les arêtes d'un octaèdre régulier est **744**.

Exemple III. — Le nombre des circuits de la figure formée par les côtés et les diagonales d'un heptagone régulier est 129 976 320, si l'on ne fragmente pas les diagonales. C'est, conformément à la règle, le nombre

---

[1] *Bulletin de l'Association française pour l'avancement des Sciences.* Congrès de Nancy (1885).

des dispositions circulaires des dés d'un jeu de dominos, jusqu'au double-six, sans les doubles. En intercalant les doubles, il faut multiplier le nombre précédent par 3^7, et, pour obtenir le nombre des dispositions rectilignes, il faut encore multiplier par le nombre 28 des dominos. (REISS, *Annali di Matematica*, 1876. — TARRY, *loc. cit.*)

Exemple IV. — Le nombre des circuits formés par les côtés et les diagonales de l'ennéagone régulier, sans fragmenter les diagonales, est

$$911\ 520\ 057\ 021\ 235\ 200.$$

C'est le nombre des dispositions circulaires des dés d'un jeu de dominos, jusqu'au double-huit, sans les doubles. En intercalant les doubles, il faut multiplier le résultat précédent par 4^9, et, pour obtenir le nombre des dispositions rectilignes, il faut encore multiplier par le nombre 45 des dominos.

Le nombre précédent a été calculé en moins de trente heures par M. G. TARRY et aussi par M. l'abbé JOLIVALD. La méthode de TARRY est d'autant plus remarquable que la solution du problème de l'heptagone, donnée par REISS, et qui était alors la seule connue, comporte à elle seule 50 pages in-4° de développements. Cependant, si l'on observe que les nombres de solutions sont, pour

le pentagone..... $2^3 . 3 . 11$,
l'heptagone...... $2^{11} . 3 . 5 . 4231$,
l'ennéagone...... $2^{16} . 3^6 . 5^2 . 7 . 11 . 9911241$,

il nous semble que, malgré son extrême élégance, la méthode de TARRY n'est pas le dernier mot de la simplicité.

Exemple V. — Le nombre des circuits du réseau des n carrefours formés par les côtés et les diagonales d'un polygone régulier de $(2n+1)$ côtés est égal au nombre des tracés en n traits et en n sauts de la figure formée par les côtés et les diagonales d'un polygone régulier de $2n$ côtés.

Exemple VI. — Le nombre des circuits d'un système de n circonférences égales, tangentes entre elles, et dont les centres sont les sommets d'un polygone régulier de n côtés, est égal au nombre des manières de tracer deux fois, sans omission, les côtés d'un polygone de n côtés.

En désignant ce nombre par R_n, la suppression d'un carrefour donne la formule

$$\frac{R_n}{2^n} = \frac{R_{n-1}}{2^{n-1}} + 1, \qquad \text{avec} \qquad \frac{R_2}{2^2} = 3,$$

par suite

$$R_n = (n+1)\,2^n.$$

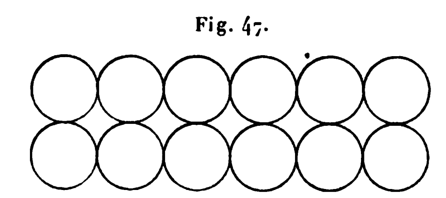
Autrement (¹). — Si l'on observe qu'un cercle étant décrit dans son

(¹) *Voir* notre article de la *Nature*, 1885.

entier on ne peut en décrire en entier qu'un autre voisin dans un circuit complet, on ramène le tracé à celui des cercles ayant leurs centres en ligne droite (n° 61, *Exemple I*). Donc, puisqu'il y a n cercles, il y a $n.2^n$ tracés. En outre, si aucun cercle n'est décrit dans son entier, on doit ajouter 2^n.

Exemple VII. — Si l'on désigne par $2^n U_{2n}$ le nombre des circuits formés par $2n$ circonférences tangentes (*fig.* 47) et par $2^{2n+1} U_{2n+1}$

Fig. 47.



le nombre des circuits formés par $(2n+1)$ circonférences (*fig.* 48), on a les deux formules

$$U_{2n} = U_{2n-1} + U_{2n-2},$$
$$U_{2n-1} = 3U_{2n-2} + U_{2n-3}.$$

Si l'on pose

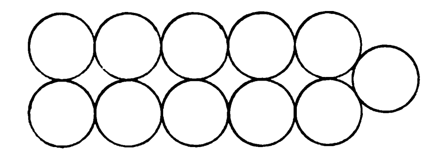
$$U_{2n} = u_n, \qquad U_{2n-1} = u_n - u_{n-1},$$

il en résulte

$$u_n = 5u_{n-1} - u_{n-2};$$

cette formule de récurrence permet de calculer U_{2n} et U_{2n-1}.

Fig. 48.



LES RÉGIONS.

63. **Les régions**. — Un point placé sur une droite indéfinie dans les deux sens la divise en deux fragments ou semi-droites; deux points d'une droite la divisent en deux fragments indéfinis et un segment fini; en général, n points d'une droite la divisent en $(n+1)$ fragments, dont deux sont indéfinis. Donc, si l'on désigne par S le nombre des points, par A le nombre des segments finis

et indéfinis, par a le nombre des segments finis et par α le nombre des segments indéfinis, on a

$$A = a + \alpha, \qquad S = A - 1,$$
$$\alpha = 2, \qquad S = a + 1.$$

Une droite illimitée, tracée dans un plan, le divise en deux régions indéfinies, c'est-à-dire en deux parties telles qu'on ne peut aller d'un point de l'une à un point de l'autre sans rencontrer la droite, à la condition de ne pas sortir du plan. Des droites parallèles, en nombre p, divisent le plan en $(p+1)$ régions indéfinies. Ces régions peuvent être garnies de deux couleurs, de telle sorte que deux régions voisines soient de couleurs différentes.

Un système de droites concourantes et indéfinies divise le plan en un nombre de régions indéfinies égal au double du nombre des droites concourantes. Ces régions peuvent être recouvertes de deux couleurs, de telle sorte que, de part et d'autre de chaque ligne de séparation, les couleurs soient différentes. Mais ceci n'aurait pas lieu pour un nombre impair de semi-droites issues d'un point.

L'ensemble de p droites parallèles et d'une transversale divise le plan en $2(p+1)$ régions illimitées. Deux systèmes formés de p droites parallèles, et de q droites parallèles, divisent le plan en $(p+1)\,(q+1)$ régions, parmi lesquelles $2(p+q)$ sont illimitées. Comme l'échiquier, on peut encore les garnir de couleurs, de telle sorte que, de part et d'autre de chaque ligne de séparation, les couleurs soient différentes.

Si l'on prolonge les côtés d'un triangle, le plan est divisé par les trois droites en sept régions, dont six sont illimitées et une seule finie, qui est l'intérieur du triangle.

Si l'on prolonge les côtés d'un quadrilatère quelconque, concave ou convexe, on forme onze régions, dont huit sont illimitées.

Lorsque l'on considère un plus grand nombre de droites, il faut tenir compte en même temps des points de concours et des segments; nous prendrons les notations suivantes :

Nombre des segments	finis..................	a
	indéfinis..............	α
	finis et indéfinis.......	A
Nombre des régions	finies..................	f
	indéfinies.............	φ
	finies et indéfinies.....	F

On a d'abord, par définition

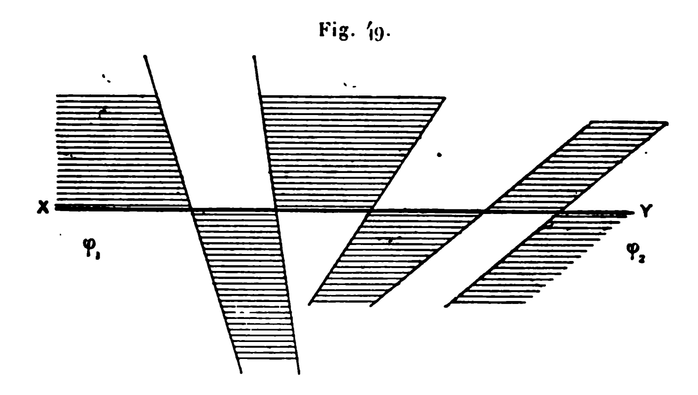
$$A = a + \alpha, \qquad F = f + \varphi.$$

Cela posé, si l'on considère n droites d'un plan, non parallèles deux à deux, et telles que trois quelconques d'entre elles ne soient pas concourantes, on a, en désignant par S le nombre des points d'intersection,

$$S = C_n^2, \qquad A = n^2, \qquad F = 1 + n + C_n^2,$$
$$\alpha = 2n, \qquad \varphi = 2n.$$

En effet, supposons ces formules démontrées pour un système de n droites, et calculons les accroissements des cinq quantités S, A, α, F, φ, lorsque l'on trace une nouvelle droite non parallèle à l'une quelconque des précédentes, et ne passant par aucun point

Fig. 49.



de concours. Nous supposerons d'abord que la droite XY a été tracée, de telle sorte que tous les points d'intersection des premières droites sont d'un même côté de XY. On observe : 1° que S augmente du nombre n des points situés sur XY; 2° que α augmente des deux segments indéfinis de cette droite; 3° que A augmente de $(2n + 1)$, c'est-à-dire des $(n + 1)$ segments finis et indéfinis de XY, et des n segments finis des droites qui aboutissent à XY; 4° que φ augmente des deux régions φ_1 et φ_2; 5° que F augmente de ces deux régions et en outre des $(n - 1)$ régions finies situées au-dessous de XY. Ainsi les formules précédentes sont générales.

On voit encore que l'adjonction de XY permet de recouvrir les régions situées au-dessus de XY de deux couleurs seulement, et toujours de telle sorte que deux régions adjacentes à un même segment soient garnies de couleurs différentes ; il suffit, en effet, d'ajouter au-dessus de XY la couleur, qui est contraire à celle de la région du dessous. En outre, il est facile de voir que les résultats précédents subsistent lorsque la droite XY se déplace et traverse le point de concours de deux droites. Nous ferons d'ailleurs observer que ces résultats s'étendent à des figures tracées sur le plan, ou sur une surface simple indéfinie dans tous les sens (comme le paraboloïde hyperbolique), pour lesquelles les droites sont remplacées par des traits indéfinis dans les deux sens, tels que chaque trait ne se recourbe pas sur lui-même. Deux traits indéfinis, qui ne se rencontrent pas, seront considérés comme des droites parallèles ; de plus, on suppose que deux traits indéfinis ne peuvent se rencontrer qu'en un seul point de concours, en se traversant mutuellement.

Nous allons étudier les modifications à apporter aux formules précédentes lorsque p droites viennent concourir en un même point, ou lorsque q droites deviennent parallèles.

1° Lorsque p droites viennent concourir en un même point, le nombre des points de concours diminue évidemment de $(C_p^2 - 1)$, puisque le nombre des points d'intersection de ces droites ne compte plus que pour 1. Les nombres φ et α des régions et des segments indéfinis ne changent pas ; le nombre A des segments finis et indéfinis diminue de $(p^2 - 2p)$, et le nombre F des régions finies et indéfinies diminue de $(1 - p + C_p^2)$.

2° Lorsque q droites deviennent parallèles, le nombre des points de concours diminue de C_q^2 ; le nombre total F des régions diminue aussi de C_q^2, et le nombre A des segments finis et indéfinis diminue de $(q^2 - q)$.

Par conséquent, si l'on désigne par σ_1 le nombre des droites de direction unique, par σ_q le nombre des groupes de q droites parallèles, par S_p le nombre des groupes de p droites concourantes, on a

$$n = \sigma_1 + 2\sigma_2 + 3\sigma_3 + \ldots + q\sigma_q + \ldots \tag{1}$$

et

$$S = S_1 + S_2 + S_3 + \ldots + S_p + \ldots . \tag{2}$$

Lorsque toutes les droites ont des directions différentes, on a $S = C_n^2$; donc, en tenant compte des diminutions,

$$(3) \quad \left\{ \begin{aligned} C_n^2 = {} & S_2 + 3S_3 + \ldots + C_p^2 S_p + \ldots \\ & + \sigma_2 + 3\sigma_3 + \ldots + C_p^2 \sigma_p + \ldots \end{aligned} \right.$$

et

$$(4) \quad \left\{ \begin{aligned} A = {} & 2S_2 + 3S_3 + \ldots + pS_p + \ldots \\ & + \sigma_1 + 2\sigma_2 + \ldots + p\sigma_p + \ldots . \end{aligned} \right.$$

On peut démontrer directement cette dernière formule en observant que, de chaque point de concours de p droites, partent $2p$ segments et que, pour toute direction de q droites parallèles, il y a $2q$ segments infinis, comptés deux fois.

Si l'on calcule F, on trouve la relation

$$(5) \qquad S + F = A + 1,$$

que l'on peut vérifier *a posteriori*. Enfin, si F_p est le nombre des régions à p frontières (ou arêtes), on a les deux formules

$$(6) \qquad F = F_1 + F_2 + F_3 + \ldots + F_p + \ldots .$$

$$(7) \qquad 2A = F_1 + 2F_2 + \ldots + pF_p + \ldots .$$

Exemple I. — Soient p points tels que trois d'entre eux ne soient pas en ligne droite, et quatre d'entre eux sur deux droites parallèles; les droites qui les joignent se rencontrent en $3C_p^4$ nouveaux points (n° 57, *Exemple I*).

Le nombre des segments finis sur chaque droite est $(C_{p-2}^2 + 3)$; le nombre total des segments est

$$A = C_p^2 C_{p-2}^2 + 3C_p^2.$$

On en tire, par la formule (5), le nombre total des régions

$$F = C_p^2 C_{p-2}^2 + 3C_p^2 + 1 - p - 3C_p^4,$$

c'est-à-dire

$$F = \tfrac{1}{8}(p-1)(p^3 - 5p^2 + 18p - 8).$$

Autrement. — Le nombre des lignes de jonction est $n = C_p^2$; le nombre des régions est

$$F = 1 + n + C_n^2 - p[1 - (p-1) + C_{p-1}^2],$$

parce que les droites se coupent au nombre de $(p-1)$ en p points. Après simplification, on retrouve le résultat précédent.

Exemple II. — Un système de n circonférences partage le plan en $n(n-1)+2$ régions, au plus, dont une seule est illimitée.

Exemple III. — Si l'on trace dans le plan n systèmes de circonférences concentriques contenant respectivement $c_1, c_2, \ldots, c_n$ circonférences, et si l'on pose

$$B = \Sigma c_1 c_2,$$

le plan est partagé en $(2B+1)$ régions, au plus, dont une seule est illimitée.

Exemple IV. — Si l'on trace, dans un plan, n systèmes de circonférences concentriques, et b circonférences non concentriques deux à deux, le plan sera partagé en régions dont le nombre est au plus

$$2\Sigma c_1 + (b-1) + 2,$$

Les trois théorèmes précédents s'appliquent aux sphères de l'espace.

Exemple V. — Si l'on trace, dans un plan, n systèmes de parallèles contenant respectivement $a_1, a_2, \ldots, a_n$ droites, et m systèmes de circonférences concentriques contenant respectivement $c_1, c_2, \ldots, c_m$ circonférences, et si l'on pose

$$A = \Sigma a_1, \qquad A' = \Sigma c_1,$$
$$B = \Sigma a_1 a_2, \qquad B' = \Sigma c_1 c_2,$$

le plan est partagé en

$$1 + A + B + 2AA' + 2B'$$

régions au plus, et le nombre des régions illimitées ne peut surpasser $2B$.

Exemple VI. — Si l'on ajoute b droites et d circonférences quelconques, le nombre précédent augmente de

$$C_b^2 + 2C_d^2.$$

Les cinq théorèmes précédents sont dus à STEINER.

64. Le problème des quatre couleurs. — Les formules que nous venons d'établir dans le numéro précédent supposent que toutes les lignes tracées dans un plan sont illimitées dans les deux sens; alors deux couleurs suffisent pour garnir la carte, de telle sorte que deux régions séparées par une ligne soient recouvertes de couleurs différentes. Il y a lieu de reprendre ces formules, lorsque le plan est divisé d'une manière quelconque par des droites et des courbes. On parvient ensuite à la démonstration de ce théorème, proposé pour la première fois par GUTHRIE, puis par DE MORGAN : *Quel que soit le mode de division d'une carte ou d'un*

globe, représentant la Terre ou un continent, en états, territoires, districts, départements, il suffit de quatre couleurs pour colorier cette carte, avec cette seule condition que deux districts ayant une limite commune soient recouverts de deux couleurs différentes. La première démonstration de cette proposition a été donnée par M. Kempe, en 1880, dans l'*American Journal* de Sylvester. Pour plus de détails, *voir* notre article de la *Revue scientifique* du 7 juillet 1883, intitulé : *Le problème géographique des quatre couleurs.*

M. Tait, professeur à l'Université d'Édimbourg, a publié là-dessus plusieurs considérations fort ingénieuses. Si l'on considère un réseau dont les carrefours ne contiennent que des points triples, ces points tous impairs sont en nombre pair, et l'on dit que le réseau possède un *isthme,* lorsque la suppression du chemin correspondant désagrège le réseau. Cela posé, on a le théorème suivant : *Dans tout réseau à n points triples, sans isthmes, on peut partager les* 3*n chemins en trois groupes de n chemins, de telle sorte que les trois chemins qui aboutissent à un même carrefour appartiennent à trois groupes différents.*

La démonstration de ce théorème se déduit immédiatement de la proposition de Guthrie ; cependant, il y aurait un grand intérêt à trouver une démonstration directe et rigoureuse du théorème de Tait. Mais, dit l'auteur, « d'après l'expression de l'éminent mathématicien Kirkmann, que j'ai consulté sur ce sujet, le *théorème présente cet irritant intérêt qu'il se joue aussi bien du doute que de la preuve* » ([1]).

LES POLYÈDRES.

65. Les polyèdres convexes. — On a le théorème suivant ([2]) : *Dans tout polyèdre convexe, le nombre des arêtes augmenté*

([1]) Tait, *Note on a theorem in Geometry of position,* dans les *Transactions of the Royal Society* (1880). Listing's *Topologie, Introductory address in the Edinburgh math. Society,* nov. 1883, et *Philos. Magaz.,* 1884. — *Reprint of math. papers from the Educational Times;* 1881, p. 113.

([2]) Ce théorème remarquable est habituellement attribué à Euler (*Novi Commentarii Petrop.,* 1752) ; mais on le trouve dans les *Œuvres inédites* de Descartes, publiées par Foucher de Careil (t. II, p. 214; Paris, 1860). La démonstration du texte est due à Cauchy.

de 2 est égal au nombre des faces augmenté du nombre des sommets.

En d'autres termes, si l'on désigne par A, F, S les nombres des arêtes, des faces et des sommets du polyèdre, on a l'égalité

$$(1) \qquad F + S = A + 2.$$

Considérons d'abord une surface polyédrale, convexe et ouverte, terminée à une ligne brisée plane ou gauche. Si l'on conserve les notations précédentes, les éléments analogues de cette surface vérifient l'égalité

$$F + S = A + 1.$$

En effet, cette formule a lieu pour une seule face; car, pour un polygone, $F = 1$ et $S = A$. Il suffit donc de montrer que la formule, étant vérifiée dans le cas de F faces, l'est encore dans le cas de $(F + 1)$ faces. Pour cela, modifions la ligne brisée qui termine la surface polyédrale, en adaptant un polygone de n côtés. Si cette face laisse toujours la surface ouverte, son périmètre ne pourra coïncider entièrement avec celui de la ligne terminale primitive. Si elle possède avec cette face p arêtes communes, elle a avec elle $(p + 1)$ sommets communs. En désignant par A′, F′, S′ les nombres des arêtes, des faces et des sommets de cette nouvelle surface polyédrale, on aura donc

$$F' = F + 1, \qquad S' = S + n - (p + 1), \qquad A' = A + n - p,$$

d'où l'on tire

$$F' + S' = A' + 1.$$

Cela posé, revenons au cas d'un polyèdre convexe. Pour obtenir une surface polyédrale, il suffit d'enlever une face, ce qui ne modifie pas les nombres A et S; donc la relation (1) est démontrée.

Si l'on désigne par f_p le nombre des faces à p arêtes, par s_p le nombre des sommets des angles polyèdres à p arêtes, on a les formules

$$\begin{aligned} F &= f_3 + f_4 + \ldots + f_p + \ldots, \\ S &= s_3 + s_4 + \ldots + s_p + \ldots, \\ 2A &= 3f_3 + 4f_4 + \ldots + pf_p + \ldots, \\ 2A &= 3s_3 + 4s_4 + \ldots + ps_p + \ldots. \end{aligned}$$

On déduit facilement des précédentes

$$2F = 4 + s_3 + 2s_4 + 3s_5 + \ldots,$$
$$2S = 4 + f_3 + 2f_4 + 3f_5 + \ldots.$$

Exemple I. — Il n'existe aucun polyèdre convexe qui ne renferme au moins une face triangulaire ou un angle trièdre. En effet, on a la formule

$$f_3 + s_3 = 8 + (f_5 + s_5) + 2(f_6 + s_6) + \ldots.$$

Exemple II. — Il n'existe aucun polyèdre convexe dont toutes les faces aient plus de cinq arêtes. — Il n'existe aucun polyèdre convexe dont tous les angles polyèdres aient plus de cinq arêtes.

Exemple III. — L'angle droit étant pris pour unité, la somme de tous les angles d'un polyèdre convexe égale le quadruple du nombre des sommets, diminué de 2.

Exemple IV. — Trouver le nombre des diagonales d'un polyèdre convexe qui ne sont pas situées dans les faces du polyèdre.

Si l'on pose

$$L = f_3 + 2f_4 + 3f_5 + \ldots,$$
$$M = 1.3.f_3 + 2.4.f_4 + 3.5.f_5 + \ldots,$$

et si l'on désigne par D le nombre des diagonales, on a

$$8D = (L + 2)(L + 4) - 4M.$$

Exemple V. — Le nombre des régions formées par n plans, tels que deux ne soient pas parallèles, que trois quelconques d'entre eux ne soient pas parallèles à une même droite, et que quatre ne passent pas par un même point, est

$$1 + C_n^1 + C_n^2 + C_n^3;$$

les régions finies sont en nombre C_{n-1}^3.

Exemple VI. — Si $p_1, p_2, \ldots, p_n$ désignent les nombres de plans parallèles de n systèmes, et si l'on pose

$$A = \Sigma p_1, \qquad B = \Sigma p_1 p_2, \qquad C = \Sigma p_1 p_2 p_3,$$

le nombre des régions de l'espace formées par ces n systèmes est égal à

$$1 + A + B + C;$$

parmi ces régions, $(2B + 2)$ sont illimitées, et les autres forment des volumes finis.

Exemple VII. — Le système formé par p plans quelconques et q sphères partage l'espace en un nombre de régions au plus égal à

$$1 + C_p^1 + C_p^2 + C_p^3 + pq(p - 1) + 2q + 2C_q^3.$$

Les régions illimitées sont en nombre $2 + 2p(p - 1)$.

Exemple VIII. — Si l'on considère des systèmes de plans parallèles en

nombres $p_1, p_2, p_3, \ldots$, et de sphères concentriques en nombres q_1, q_2, $q_3, \ldots$, et si l'on pose

$$A = \Sigma p_1, \quad B = \Sigma p_1 p_2, \quad C = \Sigma p_1 p_2 p_3,$$
$$A' = \Sigma q_1, \quad B' = \Sigma q_1 q_2, \quad C' = \Sigma q_1 q_2 q_3,$$

cet ensemble divise l'espace en un nombre de régions qui ne surpasse pas

$$1 + A + B + C + 2(AB' + BA') + 2A' + 2C'.$$

Le nombre des régions illimitées est $(2B + 2)$.

Les quatre exercices précédents sont dus à STEINER. — *Voir* une Note de M. LAISANT intitulée : *Régions du plan et de l'espace* (Congrès d'Alger, 1881).

66. **Les polyèdres convexes réguliers.** — *Il ne peut exister que cinq espèces de polyèdres convexes dont toutes les faces aient le même nombre n de côtés et dont tous les angles polyèdres aient le même nombre m d'arêtes.*

En effet, on a, par hypothèse,

$$2A = nF = mS;$$

par suite, la formule de DESCARTES donne

$$F = \frac{4m}{2(m+n) - mn}.$$

Puisque m doit être entier et positif, on ne peut faire que les hypothèses suivantes, renfermées dans le Tableau ci-après, dans lequel D désigne le nombre des diagonales.

Fig. 50.

n.	*m*.	F.	S.	A.	D.	
3	3	4	4	6	0	Tétraèdre.
3	4	8	6	12	3	Octaèdre.
3	5	20	12	30	36	Icosaèdre.
4	3	6	8	12	4	Hexaèdre.
5	3	12	20	30	100	Dodécaèdre.

Les polyèdres réguliers.

REMARQUE. — Nous ne développerons pas davantage, pour le moment, ces études sur la Géométrie de situation; cependant il y a lieu de rappeler les travaux de POINSOT, CAUCHY et BERTRAND sur les *Polyèdres étoilés;* ceux de M. CATALAN, sur les *Polyèdres semi-réguliers,* considérés d'abord par ARCHIMÈDE; ceux de BRAVAIS, sur la *Cristallographie* et sur la *Phyllotaxie;* ceux de M. CAYLEY sur les *Arbres géométriques* et leur emploi dans la théorie des combinaisons chimiques.

Dans deux importants Mémoires, trop ignorés aujourd'hui, LISTING a posé les principes généraux de la Géométrie de situation. Ses *Vorstudien zur Topologie* (1847) ont été l'objet d'un rapport sommaire dans le *Traité d'Électricité et de Magnétisme* de CLERK MAXWELL, et d'un exposé élémentaire par M. CAYLEY, dans le *Messenger of Mathematics* (1873). Dans son Mémoire de 1861, *Der Census raümlicher Complexe,* LISTING s'occupe de la formation et de la classification des nœuds; cette idée a été reprise dans plusieurs Mémoires présentés à la Société royale des Sciences d'Edimbourg, par M. TAIT, qui a retrouvé la plupart des résultats de LISTING, à propos de l'idée de THOMSON sur les *vortex-atoms.* La *Géométrie des nœuds* est un des chapitres de la Géométrie du tissage; nous exposerons, dans le second volume de cet Ouvrage, les lois arithmétiques de la Géométrie des tissus à fils rectilignes.

Exemple I. — Les hélices paradromes. — Considérons un long ruban étroit ou une bande de papier, dont les bords sont garnis d'une petite ligne noire ou d'un *liséré.* Si l'on réunit ensemble les deux extrémités, sans torsion du ruban, on forme une surface composée de deux faces et de deux liserés; on ne peut aller d'un point de l'une des faces à un point de l'autre, en cheminant sur le ruban, sans traverser l'un des lisérés. Si l'on coupe le ruban suivant sa longueur, on en obtient deux autres séparés.

Il n'en est plus ainsi lorsque l'on réunit les deux extrémités du ruban, après avoir effectué n demi-torsions dans un même sens : 1° Lorsque n est un nombre pair, la surface a encore deux faces et deux lisérés formant chacun un circuit fermé; si l'on coupe le ruban dans sa longueur, il se trouve divisé en deux autres possédant chacun n demi-torsions, comme le ruban primitif; mais les deux demi-rubans ne peuvent être séparés l'un de l'autre et se trouvent noués $\frac{1}{2}n$ fois. 2° Lorsque le nombre n des demi-torsions est impair, la surface ne présente qu'une seule face et qu'un seul liséré; si l'on coupe le ruban dans sa longueur, le ruban reste unique avec $2n$ demi-torsions, et, pour $n > 1$, il est *noué.*

Ces curieux résultats sont tirés de la *Topologie* de LISTING; ils ont été la base d'un opuscule qui eut un grand succès à Vienne, il y a quelques années, et dans lequel il s'agissait de montrer que l'on pouvait, sans escamotage ou spiritisme, exécuter le célèbre tour de faire un *nœud avec une corde sans fin*.

Au lieu de faire une seule coupe longitudinale du ruban, on peut en faire deux, trois, ..., et l'on obtient d'autres résultats.

Exemple II. — La bande de timbres-poste. — De combien de manières peut-on replier, sur un seul, une bande de p timbres-poste?

Exemple III. — La feuille de timbres-poste. — De combien de manières peut-on replier, sur un seul, une feuille rectangulaire de pq timbres-poste?

Nous ne connaissons aucune solution de ces deux problèmes difficiles proposés par M. EM. LEMOINE.

CHAPITRE VIII.

LA MULTIPLICATION ALGÉBRIQUE.

67. **Multiplication des polynômes.** — Multiplication des monômes; — d'un polynôme par un monôme; — de deux polynômes. — Règle des signes.

Le produit de plusieurs polynômes peut toujours être remplacé par un polynôme unique qu'on appelle le *produit effectué*. On opère habituellement comme il suit : on multiplie successivement tous les termes du premier polynôme, en commençant par la gauche, par le premier, le second, ..., le dernier terme du second polynôme. On obtient ainsi un premier produit partiel; on fait, s'il y a lieu, la réduction des termes semblables. On multiplie ensuite chacun des termes du produit partiel successivement par le premier, le second, ..., le dernier terme du troisième polynôme, en commençant toujours par la gauche, et ainsi de suite.

Le produit des polynômes A, B, C, ..., L est la somme de tous les produits de n facteurs formés avec un terme de A, un terme de B, ..., et un terme de L; s'il n'y a aucune réduction, le nombre des termes du produit est égal au produit des nombres des termes des facteurs.

Soit, en général,

$$\begin{aligned} A &= a_1 + a_2 + a_3 + \ldots + a_\alpha, \\ B &= b_1 + b_2 + b_3 + \ldots + b_\beta, \\ C &= c_1 + c_2 + c_3 + \ldots + c_\gamma, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Pour faire la multiplication des polynômes A, B, C, ..., on multiplie tous les termes de A successivement par tous ceux de B pris dans l'ordre de gauche à droite; puis on multiplie tous les termes du produit par ceux de C, et ainsi de suite. Un terme quelconque a une expression de la forme $a_{\alpha'} b_{\beta'} c_{\gamma'} \ldots$, en désignant

par α' l'un des entiers 1, 2, ..., α, et de même pour β' et pour γ'. Dans le produit total, les termes pris dans l'ordre successif sont d'abord ceux qui ne contiennent que a, en nombre α; puis ceux qui ne contiennent que a ou b, pris séparément ou simultanément; ils sont en nombre $\alpha\beta$; puis les termes du produit par C qui sont en nombre $\alpha\beta\gamma$, et ainsi de suite. On voit ainsi que le rang du terme $a_{\alpha'} b_{\beta'} c_{\gamma'} d_{\delta'}$ est fourni par l'expression

$$n = \alpha\beta\gamma\delta' + \alpha\beta\gamma' + \alpha\beta' + \alpha'.$$

Inversement, lorsque n est donné, on observe que δ' est l'entier de la division de n par $\alpha\beta\gamma$, que γ' est l'entier de la division du reste par $\alpha\beta$, et ainsi de suite. En particulier, si $\alpha = \beta = \gamma = \delta$, la détermination du terme qui correspond à un rang donné n revient à écrire n dans le système de numération de base α.

Ainsi, dans le produit

$$(1-a)(1-b)\ldots(1-l),$$

pour avoir le signe du terme de rang n, on écrit ce nombre n dans le système de numération binaire; le terme correspondant est positif, ou négatif, suivant que le nombre des 1, et celui des 0 qui terminent n, sont, ou ne sont pas, de même parité.

Carré d'un polynôme. — Interprétation géométrique :

$$(a+b+c+\ldots+l)^2 = \Sigma a^2 + 2\Sigma ab.$$

Cube d'un polynôme. — Interprétation géométrique :

$$(\Sigma a)^3 = \Sigma a^3 + 3\Sigma a^2 b + 6\Sigma abc.$$

Quatrième puissance d'un polynôme. — On a la formule

$$(\Sigma a)^4 = \Sigma a^4 + 4\Sigma a^3 b + 6\Sigma a^2 b^2 + 12\Sigma a^2 bc + 24\Sigma abcd.$$

On trouvera plus loin la formule générale qui donne le développement de la puissance d'un polynôme.

Exemple I. — Si l'on désigne respectivement par A, B, C, D les polynômes

$$a-b-c,\quad b-c-a,\quad c-a-b,\quad a+b+c,$$

on a les formules

$$A + B + C + D = 0,$$
$$A^2 + B^2 + C^2 + D^2 = 4\Sigma a^2,$$
$$A^3 + B^3 + C^3 + D^3 = 24abc,$$
$$A^4 + B^4 + C^4 + D^4 = 4\Sigma a^4 + 24\Sigma a^2b^2,$$
$$A^5 + B^5 + C^5 + D^5 = 80abc.\Sigma a^2,$$
$$A^7 + B^7 + C^7 + D^7 = 56abc(3\Sigma a^4 + 10\Sigma a^2b^2),$$
$$ABCD = \Sigma a^4 - 2\Sigma a^2b^2.$$

Exemple II. — Si l'on désigne par A, B, C, D les polynômes

$$b + c + d - a,\quad c + d + a - b,\quad d + a + b - c,\quad a + b + c - d,$$

et par P, Q, R, S les polynômes

$$a + b + c + d,\quad a + b - c - d,\quad b + c - a - d,\quad c + a - b - d,$$

les valeurs de l'expression

$$P^n + Q^n + R^n + S^n - A^n - B^n - C^n - D^n$$

sont

pour $n = 2$........... 0,
» $n = 4$........... $192abcd$,
» $n = 6$........... $960abcd.\Sigma a^2$,
» $n = 8$........... $896abcd(3\Sigma a^4 + 10\Sigma a^2b^2)$.

Exemple III. — En conservant les notations de l'Exemple précédent, on a la formule

$$ABCDPQRS = \Sigma a^8 - 4\Sigma a^6b^2 + 6\Sigma a^4b^4 + 4\Sigma a^4b^2c^2 - 40a^2b^2c^2d^2.$$

Exemple IV. — Développer le produit des seize facteurs

$$a \pm b \pm c \pm d \pm e.$$

Si l'on remplace, dans l'*Exemple III*, le nombre d par $(d + e)$, puis par $(d - e)$, et si l'on multiplie les résultats obtenus, on trouve

$$\Sigma a^{16} - 8\Sigma a^{14}b^2 + 28\Sigma a^{12}b^4 + 40\Sigma a^{12}b^2c^2$$
$$- 56\Sigma a^{10}b^6 - 72\Sigma a^{10}b^4c^2 - 176\Sigma a^{10}b^2c^2d^2$$
$$+ 70\Sigma a^8b^8 + 40\Sigma a^8b^6c^2 + 36\Sigma a^8b^4c^4 + 344\Sigma a^8b^4c^2d^2 - 752\Sigma a^8b^2c^2d^2e^2$$
$$+ 16\Sigma a^6b^6c^4 - 416\Sigma a^6b^6c^2d^2 - 272\Sigma a^6b^4c^4d^2 + 928\Sigma a^6b^4c^2d^2e^2$$
$$+ 2008\Sigma a^4b^4c^4d^4 - 1520\Sigma a^4b^4c^4d^2e^2.$$

Cette méthode de calcul est due à DESCARTES.

68. Le carré magico-magique de Fermat. — Avec deux groupes de quatre nombres a, b, c, d, et p, q, r, s, on forme une table d'addition à deux entrées, comme celle de Pythagore (*fig.* 51).

Fig. 51.

$$\begin{array}{cccc} a+p, & b+p, & c+p, & d+p, \\ a+q, & b+q, & c+q, & d+q, \\ a+r, & b+r, & c+r, & d+r, \\ a+s, & b+s, & c+s, & d+s. \end{array}$$

Table d'addition.

En permutant les lignes, ou les colonnes, ou en échangeant les lignes et les colonnes, on forme $2(1.2.3.4)^2 = 1152$ tables distinctes. Si l'on prend quatre nombres d'une table, de telle sorte qu'il n'y en ait pas deux dans la même ligne ou dans la même colonne, on obtient une somme évidemment égale à celle des huit nombres donnés. Pour chaque table, il existe ainsi vingt-quatre sommes constantes, en nombre égal aux permutations figurées de quatre objets (n° 43).

Échangeons deux à deux les huit nombres placés symétriquement par rapport au centre du carré, et qui ne sont pas situés sur les diagonales; puis, échangeons deux quartiers opposés de quatre termes, l'inférieur à gauche et le supérieur à droite; nous formons ainsi le Tableau que l'on appelle carré magico-magique.

Fig. 52.

$$\begin{array}{cccc} a+p, & c+s, & d+q, & b+r, \\ d+r, & b+q, & a+s, & c+p, \\ b+s, & d+p, & c+r, & a+q, \\ c+q, & a+r, & b+p, & d+s. \end{array}$$

Carré magico-magique.

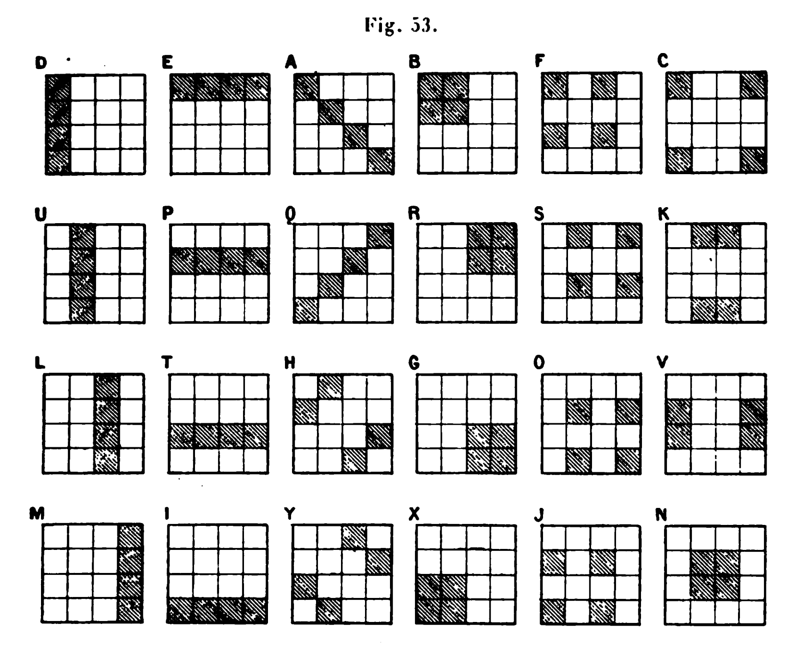
Si l'on fait la même transformation sur les permutations figurées, on trouve la *fig.* 53. Par suite, la somme des quatre nombres du carré magique qui correspondent à quatre cases grises de cette figure est constante. Il y a donc 1152 carrés magico-magiques.

On peut tripler ce nombre lorsque

$$a+d=b+c \quad \text{et} \quad p+s=q+r.$$

comme cela a lieu pour les deux groupes 1, 2, 3, 4, et 0, 4, 8, 12, qui reproduisent les seize premiers nombres. Dans ce cas, on a les théorèmes suivants : Dans tout carré magico-magique, la somme

Fig. 53.



Les vingt-quatre sommes constantes d'un carré magico-magique.

des huit nombres placés dans les deux diagonales égale la somme des huit autres. Il en est de même pour la somme des carrés et pour la somme des cubes (¹).

69. Formules d'Euler pour les produits des sommes de quatre carrés. — On a l'identité

$$(a^2 + b^2)(p^2 + q^2) = (ap - bq)^2 + (aq + bp)^2,$$

indiquée par Fibonacci ; elle exprime que *le produit d'une somme de deux carrés par une somme de deux carrés est une somme de deux carrés*. En changeant le signe de p, on obtient, dans le

(¹) Voir notre article du *Journal de Mathématiques élémentaires*, 1887, intitulé : *Les carrés magiques de* Fermat *et de* Frénicle.

cas général, une autre décomposition; mais, si $a = p$, $b = q$, on a la décomposition unique

$$(a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2,$$

qui est la formule fondamentale des *triangles rectangles en nombres*, dont la théorie sera exposée plus loin.

La formule précédente a été généralisée par Euler qui a donné le théorème suivant : *Le produit d'une somme de quatre carrés par une somme de quatre carrés est une somme de quatre carrés.* En effet, si l'on remplace les sommes par des produits dans le carré magique du numéro précédent, et si l'on donne le signe — aux termes de la première diagonale, on trouve que la somme des expressions

$$\begin{aligned} &(-ap + cs + dq + br)^2 \\ +&(+dr - bq + as + cp)^2 \\ +&(+bs + dp - cr + aq)^2 \\ +&(+cq + ar + bp - ds)^2 \end{aligned}$$

égale le produit des deux sommes de quatre carrés

$$(a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2).$$

En permutant p, q, r, s, on a vingt-quatre formules distinctes; puis, en changeant le signe de p, on en obtient vingt-quatre autres. Ainsi la décomposition du produit des sommes de quatre carrés en quatre carrés se déduit très facilement de la considération des carrés magico-magiques.

Brioschi a donné des formules semblables pour le produit de deux sommes de huit carrés; mais, contrairement à ce que l'on pensait, M. Samuel Roberts a démontré qu'il n'existait pas de formules analogues pour les sommes de seize carrés, ou plus (*The Quarterly Journal*, 1879 et 1880).

D'autre part, il ne peut exister de formule semblable pour les sommes de trois carrés : ainsi 3 et 21 sont des sommes de trois carrés

$$3 = 1^2 + 1^2 + 1^2 \qquad \text{et} \qquad 21 = 4^2 + 2^2 + 1^2,$$

et leur produit 63 ne peut être décomposé en moins de quatre carrés. De même, le produit des deux formes

$$a^2 + b^2 + 2c^2, \qquad p^2 + q^2 + 2r^2$$

ne peut donner un résultat de même forme, puisque l'on a, par exemple,

$$6 = 0^2 + 2^2 + 2.1^2 \quad \text{et} \quad 13 = 1^2 + 2^2 + 2.2^2,$$

et que le produit 78 ne peut être décomposé de cette manière.

Nous démontrerons plus loin, au moyen des formules d'EULER, ce théorème énoncé par BACHET : *Tout entier est la somme de quatre carrés, ou d'un moindre nombre.*

70. Formules de Lagrange. — On a l'identité suivante

$$\begin{aligned}(a^2+\lambda b^2+\mu c^2+\lambda\mu d^2)(p^2+\lambda r^2+\mu s^2+\lambda\mu q^2)\\ =[+ap+\mu cs+\lambda\mu dq+\lambda br]^2\\ +\mu[\lambda dr-\lambda bq+as+cp]^2\\ +\lambda\mu[bs+dp-cr+aq]^2\\ +\lambda[\mu cq+ar+bp-\mu ds]^2;\end{aligned}$$

pour $\lambda = \mu = 1$, on retrouve les formules d'EULER.

On a encore cette autre identité de LAGRANGE, qui s'applique à un nombre quelconque de carrés :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2) = (ap+bq+cr+ds)^2\\ +(aq-bp)^2+(ar-cp)^2\\ +(as-dp)^2+(br-cq)^2\\ +(bs-dq)^2+(cs-dr)^2.\end{aligned}$$

On remplace ainsi le produit de sommes de n carrés par une somme de $(1+C_n^2)$ carrés, tandis que le produit effectué donne n^2 carrés.

Exemple I. — Vérifier les formules suivantes, dans lesquelles u_n désigne le terme de rang $(n+1)$ de la suite de FIBONACCI (n° 3) :

$$\begin{aligned}u_n^2 - u_{n-1}u_{n+1} = (-1)^{n-1},\\ u_{n-1}^2 + u_n^2 = u_{2n-1},\\ u_1^2+u_2^2+\ldots+u_n^2 = u_n u_{n+1},\\ u_n^3+u_{n+1}^3-u_{n-1}^3 = u_{3n},\\ u_n u_{n+1} - u_{n-2}u_{n-1} = u_{2n-1},\\ u_{n+1}u_{n+2} - u_n u_{n+3} = (-1)^n,\\ u_n^4 - u_{n-2}u_{n-1}u_{n+1}u_{n+2} = 1,\\ u_1u_2+u_2u_3+\ldots+u_{2n-1}u_{2n} = u_{2n}^2,\\ u_1u_2+u_2u_3+\ldots+u_{2n}u_{2n+1} = u_{2n+1}^2-1.\end{aligned}$$

La première des relations précédentes est due à Albert Girard; elle donne lieu à un curieux *Paradoxe géométrique* (voir nos *Récréations mathématiques*, t. II. — Cinquième Récréation).

Exemple II. — Considérons la suite récurrente donnée par la formule

$$U_{n+2} = p\,U_{n+1} - q\,U_n,$$

et par les deux premiers termes U_0 et U_1; soit, de plus, u_n le terme de rang $(n+1)$ dans une suite donnée par la même loi et dont les deux premiers termes sont $u_0 = 0$ et $u_1 = 1$; vérifier la formule

$$U_n = U_0 u_{n-1} + U_1 u_n.$$

Exemple III. — Si $p = 6q \pm 1$, on a l'identité

$$4p^2 + 1 = (8q \pm 2)^2 + (8q \pm 1)^2 + (4q)^2.$$

Exemple IV. — *Le carré et le cube d'une somme de trois carrés sont des sommes de trois carrés.* — En effet, on a

$$\begin{aligned}(x^2+y^2+z^2)^2 &= (x^2+y^2-z^2)^2+(2xz)^2+(2yz)^2,\\ (x^2+y^2+z^2)^3 &= (x^3-3xz^2-2zy^2+xy^2)^2\\ &\quad+(y^3-yx^2-yz^2+4xyz)^2\\ &\quad+(z^3-3zx^2-2xy^2+zy^2)^2.\end{aligned}$$

Plus généralement, M. Neuberg a démontré que toute puissance de

$$ax^2+by^2+cz^2$$

est un nombre de la même forme (*Mathesis*, I, p. 75).

Exemple V. — Si l'on pose

$$P = a^2+b^2+c^2-bc-ca-ab,$$

on a les identités

$$\begin{aligned}2P &= (b-c)^2+(c-a)^2+(a-b)^2,\\ 2P^2 &= (b-c)^4+(c-a)^4+(a-b)^4,\\ P^2 &= (a-b)^2(a-c)^2+(b-c)^2(b-a)^2+(c-a)^2(c-b)^2,\\ (a+b+c)P &= a^3+b^3+c^3-3abc.\end{aligned}$$

Exemple VI. — On a l'identité

$$aX^3+bY^3+a^2b^2Z^3 = V^2,$$

dans laquelle on suppose

$$\begin{aligned}X &= x(ax^3+2by^3),\\ Y &= y(by^3+2ax^3),\\ Z &= 3x^2y^2,\\ V &= a^2x^6+7abx^3y^3+b^2y^6.\end{aligned}$$

Exemple VII. — On considère le tableau des neuf quantités

$$\begin{array}{lll} p^2+q^2-r^2-s^2, & 2(qr+ps), & 2(qs-pr), \\ 2(qr-ps), & p^2+r^2-q^2-s^2, & 2(rs+pq), \\ 2(qs+pr), & 2(rs-pq), & p^2+s^2-q^2-r^2; \end{array}$$

vérifier que la somme des carrés des nombres contenus dans une même ligne ou dans une même colonne est égale au carré de $p^2+q^2+r^2+s^2$ (voir *Nouv. Corr. math.*, t. II, p. 97).

Exemple VIII. — Trouver quatre nombres tels que leurs produits deux à deux, augmentés de l'unité, soient des carrés (DIOPHANTE, liv. IV, prop. 21). — Si l'on pose

$$\begin{aligned} a &= r, \\ b &= s(rs+2), \\ c &= (s+1)(rs+r+2), \\ d &= 4(rs+1)(rs+r+1)(rs^2+rs+2s+1), \end{aligned}$$

les carrés des six expressions

$$\begin{aligned} & rs+1, \\ & rs+r+1, \\ & 2r^2s^2+2r^2s+4rs+2r+1, \\ & rs^2+rs+2s+1, \\ & 2r^2s^3+2r^2s^2+6rs^2+4rs+4s+1, \\ & 2r^2s^3+4r^2s^2+2r^2s+6rs^2+8rs+2r+4s+3 \end{aligned}$$

sont respectivement égaux aux six quantités

$$\begin{array}{lll} ab+1, & ac+1, & ad+1, \\ bc+1, & bd+1, & cd+1. \end{array}$$

Une autre solution a été donnée par EULER (*Commentationes Arithmeticæ collectæ*, t. II, p. 45).

71. Valeur numérique d'un polynôme ordonné. — Réduction des termes semblables. Ordonner un polynôme suivant les exposants croissants ou décroissants.

Pour obtenir la valeur numérique d'un polynôme

$$f(x) = p_0x^n + p_1x^{n-1} + p_2x^{n-2} + \ldots + p_n,$$

qui correspond à une valeur donnée $x = a$, on calcule successi-

vement les expressions

$$\begin{aligned}
f_0 &= p_0,\\
f_1 &= p_0 a + p_1,\\
f_2 &= p_0 a^2 + p_1 a + p_2,\\
f_3 &= p_0 a^3 + p_1 a^2 + p_2 a + p_3,
\end{aligned}$$

en déduisant chaque résultat du précédent par les formules

$$\begin{aligned}
f_1 &= af_0 + p_1,\\
f_2 &= af_1 + p_2,\\
f_3 &= af_2 + p_3,\\
f_4 &= af_3 + p_4,\\
&\dots\dots\dots\dots;
\end{aligned}$$

chacun des polynômes f_1, f_2, f_3, f_4, ..., est égal au précédent multiplié par a, et augmenté du coefficient correspondant de $f(x)$. Lorsqu'il manque des termes, on doit tenir compte des coefficients nuls.

Pour $x = 1$, le polynôme est égal à la somme de ses coefficients; pour $x = -1$, il est égal à leur somme alternée.

72. Divisibilité de $f(x)$ par $(x-a)$. — Considérons la multiplication

$$\begin{array}{l|l|l|l}
\multicolumn{4}{l}{f_0x^{n-1}+f_1x^{n-2}+f_2x^{n-3}+\dots+f_{n-1}}\\
\multicolumn{4}{l}{\quad x-a}\\
\hline
f_0x^n + f_1 & x^{n-1} + f_2 & x^{n-2} + \dots + f_{n-1} & x\\
\qquad -af_0 & \qquad -af_1 & \qquad -\dots - af_{n-2} & \quad -af_{n-1}\\
\hline
p_0x^n + p_1 & x^{n-1} + p_2 & x^{n-2} + \dots + p_{n-1} & x + p_n - f(a).
\end{array}$$

Donc, en désignant par Q le multiplicande, on a

$$f(x) = (x-a)Q + f(a);$$

par suite, *la condition nécessaire et suffisante, pour que $f(x)$ soit divisible par le binôme $(x-a)$, est $f(a) = 0$.*

Si un polynôme $f(x)$ est divisible séparément par les binômes $(x-a)$, $(x-b)$, ..., $(x-l)$, dans lesquels a, b, c, ..., l, sont des quantités inégales deux à deux, il est divisible par le produit des binômes.

Réciproquement, pour que $f(x)$ soit divisible par le produit

$$(x-a)(x-b)(x-c)\ldots(x-l),$$

dans lequel les nombres a, b, c, ..., l sont inégaux deux à deux, il faut et il suffit que l'on ait

$$f(a)=0,\quad f(b)=0,\quad f(c)=0,\quad \ldots,\quad f(l)=0.$$

73. Identité et similitude des polynômes. — Deux polynômes réduits et ordonnés sont dits *identiques* (ou *semblables*), si les coefficients des mêmes puissances de x sont égaux (ou *proportionnels*). Le nombre des conditions pour que les polynômes de degré n soient identiques est $(n+1)$, et le nombre des conditions pour qu'ils soient semblables est n.

Si un polynôme $f(x)$ de degré n s'annule pour plus de n valeurs de x inégales deux à deux, tous les coefficients de ce polynôme sont nuls, et le polynôme est nul quelle que soit la valeur de x.

Si les valeurs numériques de deux polynômes de degré n sont égales (ou proportionnelles), pour plus de n valeurs de x inégales deux à deux, les polynômes sont identiques (ou semblables).

Les opérations d'addition, de soustraction, de multiplication sur des polynômes ordonnés ne peuvent donner comme résultats que des polynômes identiques, quel que soit l'ordre des opérations.

Lorsque le multiplicande, le multiplicateur et le produit, sont ordonnés de la même manière par rapport à la variable x, le premier et le dernier terme du produit sont respectivement égaux aux produits des premiers et des derniers termes des facteurs.

Exemple I. — On a l'identité

$$x^4+4y^4=(x^2+2xy+2y^2)(x^2-2xy+2y^2).$$

Pour $y=1$, on déduit cette proposition de SOPHIE GERMAIN (1) :

Tout nombre entier (x^4+4), autre que 5, est le produit de deux nombres entiers. Pour $x=1$ et $y=2^n$, on a la formule d'AURIFEUILLE, entrevue par BÉGUELIN (2),

$$2^{4n+2}+1=(2^{2n+1}+2^{n+1}+1)(2^{2n+1}-2^{n+1}+1).$$

---

(1) *Manuscrit* n° 9118 *du fonds français de la Bibliothèque nationale* (p. 84).

(2) *Mémoires de l'Académie de Berlin* pour 1772, p. 296.

Exemple II. — On a l'identité

$$x^6 + 27y^6 = (x^2 + 3y^2)(x^2 - 3xy + 3y^2)(x^2 + 3xy + 3y^2),$$

et pour $x = 1$, $y = 3^n$, on en déduit que $3^{6n+3} + 1$ est le produit de trois facteurs.

Exemple III. — Le nombre $x^{10} - 5^5 y^{10}$ est le produit des trois facteurs

$$x^2 - 5y^2, \quad x^4 + 15x^2y^2 + 25y^4 \pm 5xy(x^2 + 5y^2).$$

Exemple IV. — Le nombre $x^{12} + 6^6 y^{12}$ est le produit des trois facteurs

$$x^4 + 36y^4, \quad x^4 + 18x^2y^2 + 36y^4 \pm 6xy(x^2 + 6y^2).$$

Ces formules sont les premières de deux longues suites de formules que nous avons tirées de deux de nos mémoires : *Théorèmes arithmétiques* (Acad. de Turin, 1878). — *Sur les formules de* Cauchy et de Lejeune-Dirichlet (*Association française*, Congrès de Paris, 1878).

Exemple V. — Si l'on pose

$$\begin{aligned} X &= x^3 - y^3 + 3xy(2x + y), \\ Y &= y^3 - x^3 + 3yx(2y + x), \\ Z &= 3(x^2 + xy + y^2), \\ A &= xy(x + y), \end{aligned}$$

on a l'identité

$$X^3 + Y^3 = AZ^3.$$

En particulier, pour $x = 1$ et $y = 2$, on a

$$17^3 + 37^3 = 6.21^3,$$

qui donne une solution de l'équation indéterminée

$$X^3 + Y^3 = 6Z^3,$$

et, par suite, une infinité de solutions, bien que Legendre ait affirmé son irrésolubilité dans sa *Théorie des Nombres* ([1]).

74. Binôme de Vandermonde. — Posons, pour simplifier,

$$(1 + x)^p = 1 + p_1 x + p_2 x^2 + \ldots + p_2 x^{p-2} + p_1 x^{p-1} + x^p;$$

on a aussi

$$(x + 1)^p = x^p + p_1 x^{p-1} + p_2 x^{p-2} + \ldots + p_2 x^2 + p_1 x + 1;$$

([1]) Voir nos *Théorèmes généraux sur l'impossibilité des équations cubiques indeterminées* (*Bulletin de la Soc. math.*, t. VIII).

en multipliant membre à membre et en égalant les coefficients de x^p, d'après la loi d'identité des polynômes, il vient

$$C_{2p}^p = 1^2 + p_1^2 + p_2^2 + \ldots + p_2^2 + p_1^2 + 1^2;$$

en d'autres termes, *la somme des carrés des coefficients du développement de* $(1+x)^p$ *égale le coefficient du milieu dans le développement de la puissance d'exposant double.*

De même, en égalant les coefficients de x^p dans le développement de $(1-x^2)^p$, d'une part, et dans le produit des développements de $(1+x)^p$ et de $(1-x)^p$, d'autre part, on trouve que *la somme alternée des carrés des coefficients du développement de* $(1+x)^p$,

$$1^2 - p_1^2 + p_2^2 - p_3^2 + \ldots + (-1)^p . 1^2,$$

est égale au coefficient du milieu de ce développement lorsque p est pair, et à zéro lorsque p est impair.

Plus généralement, on peut égaler le coefficient de x^r dans le développement de $(1+x)^{p+q}$, d'une part, et dans le produit des développements de $(1+x)^p$ et de $(1+x)^q$, d'autre part. On trouve alors une formule qui ne diffère que par la forme d'une identité donnée par Vandermonde, et que l'on appelle *binôme des factorielles* (n° 48, *Ex. IV*). En d'autres termes, le binôme des factorielles est le résultat de la loi d'identité des polynômes, que l'on obtient dans le procédé de la multiplication accélérée des polynômes ordonnés, en étendant à ceux-ci le procédé de multiplication rapporté par Fibonacci (n° 19). Ces diverses propriétés sont considérablement amplifiées dans les numéros suivants.

Exemple I. — Trouver la somme des produits deux à deux des coefficients du binôme.

Lorsque l'on connaît la somme de p nombres et la somme de leurs carrés, on obtient la somme de leurs produits deux à deux par la formule

$$2\Sigma ab = (\Sigma a)^2 - \Sigma a^2,$$

que l'on déduit du carré d'un polynôme. Dans l'exemple, on a donc

$$2\Sigma ab = 2^{2p} - \frac{(2p)!}{(p!)^2}.$$

Remarque. — On ne connaît pas de formule simple pour la somme des cubes des coefficients du binôme.

Exemple II. — Si l'on multiplie respectivement les q premiers coefficients du développement de $(1-x)^p$ par les q premiers termes d'une progression arithmétique ayant a pour premier terme et r pour raison, on a pour somme des produits

$$(-1)^{q-1}\frac{q}{p(p-1)}[pr(q-1)+a(p-1)]\,C_p^q. \quad \text{(Delannoy.)}$$

Exemple III. — Démontrer les deux formules

$$\frac{1}{n+1}C_{2n}^{n}+\frac{3}{n+2}C_{2n}^{n-1}+\ldots+\frac{2n-1}{2n}C_{2n}^{1}=C_{2n}^{n}-1,$$

$$\frac{2}{n+1}C_{2n-1}^{n-1}+\frac{4}{n+2}C_{2n-1}^{n-2}+\ldots+\frac{2n-2}{2n-1}C_{2n-1}^{1}=C_{2n-1}^{n-1}-1.$$

THÉORÈMES GÉNÉRAUX SUR LE CALCUL DES SOMMES ET DES DIFFÉRENCES.

75. Relation entre les termes d'une même ligne. — La loi de formation d'un Tableau de sommes donne (n° 5)

$$\Sigma u_1 = u_0 + \Sigma u_0,$$
$$\Sigma^2 u_1 = \Sigma u_0 + \Sigma^2 u_0;$$

par suite, en ajoutant,

$$\Sigma^2 u_2 = u_0 + 2\Sigma u_0 + \Sigma^2 u_0.$$

En passant *à la colonne suivante,* on a

$$\Sigma^3 u_2 = \Sigma u_0 + 2\Sigma^2 u_0 + \Sigma^3 u_0;$$

en ajoutant les deux dernières égalités, il vient

$$\Sigma^3 u_3 = u_0 + 3\Sigma u_0 + 3\Sigma^2 u_0 + \Sigma^3 u_0.$$

On a, par induction, la formule suivante que l'on peut vérifier *a posteriori*

$$\Sigma^p u_p = u_0 + C_p^1\Sigma u_0 + C_p^2\Sigma^2 u_0 + \ldots + \Sigma^p u_0,$$

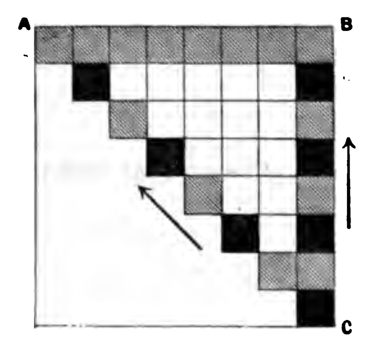
ou, sous la forme symbolique,

$$(1) \qquad \Sigma^p u_p \doteq (1+\Sigma)^p u_0;$$

on doit remplacer les exposants des puissances de Σ par des indices, et $\Sigma^0 u_0$ par u_0.

On peut augmenter d'un nombre quelconque, soit les indices de Σ, soit ceux de u; d'où l'on déduit que *si l'on multiplie respectivement* $(p+1)$ *termes consécutifs d'une ligne* AB *d'un tableau de sommes, par les coefficients du développement de* $(1+x)^p$, *on obtient, pour somme des produits, le terme* C *du Tableau, placé au-dessous de* B *dans la même colonne, et de* A, *dans la même diagonale* (*fig.* 54).

Fig. 54.



Pour le tableau des différences, la formule précédente devient

$$(1') \qquad u_p \doteq (1+\Delta)^p u_0.$$

76. Relation entre les termes d'une même colonne. — On a la formule

$$\Sigma u_0 = \Sigma^2 u_1 - \Sigma^2 u_0;$$

en passant *à la ligne suivante,*

$$\Sigma u_1 = \Sigma^2 u_2 - \Sigma^2 u_1;$$

en retranchant la première égalité de la seconde, il vient

$$u_0 = \Sigma^2 u_2 - 2\Sigma^2 u_1 + \Sigma^2 u_0.$$

En retranchant cette égalité de celle que l'on obtient en passant à la ligne suivante, il vient

$$u_0 = \Sigma^3 u_3 - 3\Sigma^3 u_2 + 3\Sigma^3 u_1 - \Sigma^3 u_0.$$

On trouve ainsi la formule générale

$$u_0 = \Sigma^p u_p - C_p^1 \Sigma^p u_{p-1} + C_p^2 \Sigma^p u_{p-2} + \ldots + (-1)^p \Sigma^p u_0,$$

ou, sous la forme symbolique,

$$(2) \qquad u_0 \triangleq \Sigma^p (u-1)^p,$$

à la condition de remplacer, après le développement de $(u-1)^p$, les exposants de u par des indices, *sans oublier l'exposant zéro.*

Par conséquent, *si l'on multiplie* $(p+1)$ *termes consécutifs d'une même colonne* CB *d'un Tableau de sommes, en remontant, par les coefficients de* $(1-x)^p$, *on trouve pour somme des produits le terme* A *du Tableau* (*fig.* 54).

Avec la notation Δ du calcul des différences, la formule précédente s'écrit

$$(2') \qquad \Delta^p u_0 \triangleq (u-1)^p.$$

77. Relation entre les termes d'une même diagonale. — On a la formule

$$\Sigma u_0 = \Sigma u_1 - u_0;$$

par suite, en passant *à la ligne et à la colonne suivantes,*

$$\Sigma^2 u_1 = \Sigma^2 u_2 - \Sigma u_1;$$

et, en retranchant membre à membre

$$\Sigma^2 u_0 = \Sigma^2 u_2 - 2\Sigma u_1 + u_0,$$

en général,

$$\Sigma^p u_0 = \Sigma^p u_p - C_p^1 \Sigma^{p-1} u_{p-1} + C_p^2 \Sigma^{p-2} u_{p-2} - \ldots;$$

ou, sous la forme symbolique,

$$(3) \qquad \Sigma^p u_0 \triangleq (\Sigma u - 1)^p.$$

Par conséquent, *si l'on multiplie respectivement* $(p+1)$ *termes consécutifs d'une diagonale* CA *d'un tableau de sommes par les coefficients du développement de* $(1-x)^p$, *on obtient pour somme des produits le terme* B *du Tableau* (*fig.* 54).

Avec la notation des différences, on a

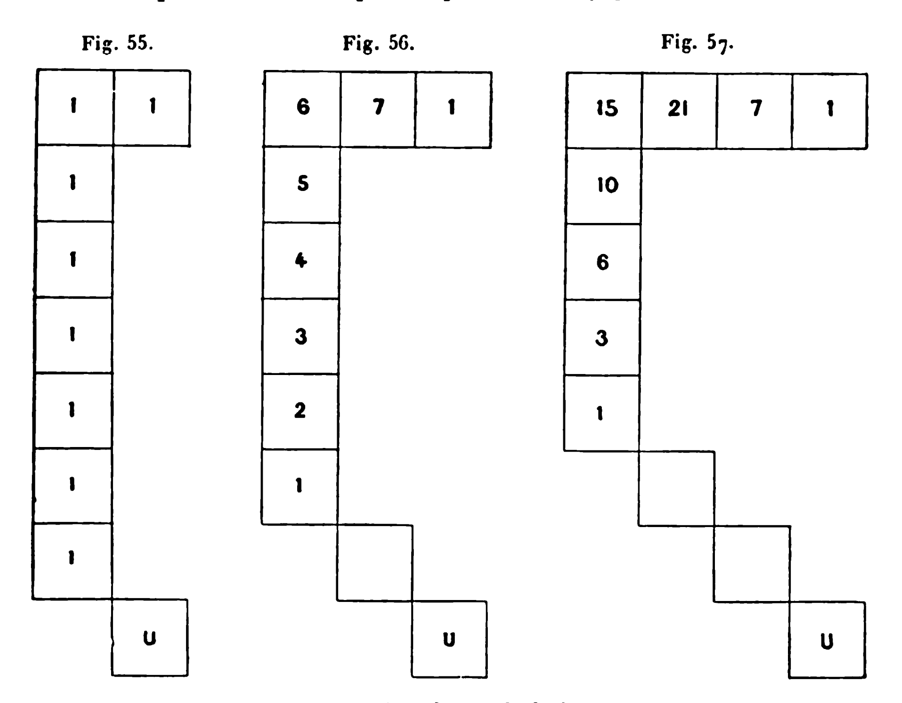
$$(3') \qquad u_0 \triangleq (u-\Delta)^p.$$

Si le tableau des u représente le triangle de PASCAL, les rela-

tions précédentes subsistent; l'une d'elles donne, en particulier, le binôme de VANDERMONDE. On peut appliquer ces relations au triangle arithmétique, en le supposant illimité dans tous les sens.

On observera que les formules (1) et (1'), (2) et (2'), (3) et (3'), rentrent deux par deux l'une dans l'autre, si l'on se rappelle l'*identité symbolique d'opération* $\Sigma\Delta = 1$, c'est-à-dire si l'on remplace Σ^p par Δ^{-p}.

78. Démonstrations figurées. — Les théorèmes que nous venons d'exposer peuvent être démontrés et généralisés par des calculs très simples d'Arithmétique de position. La *fig.* 55 nous rappelle



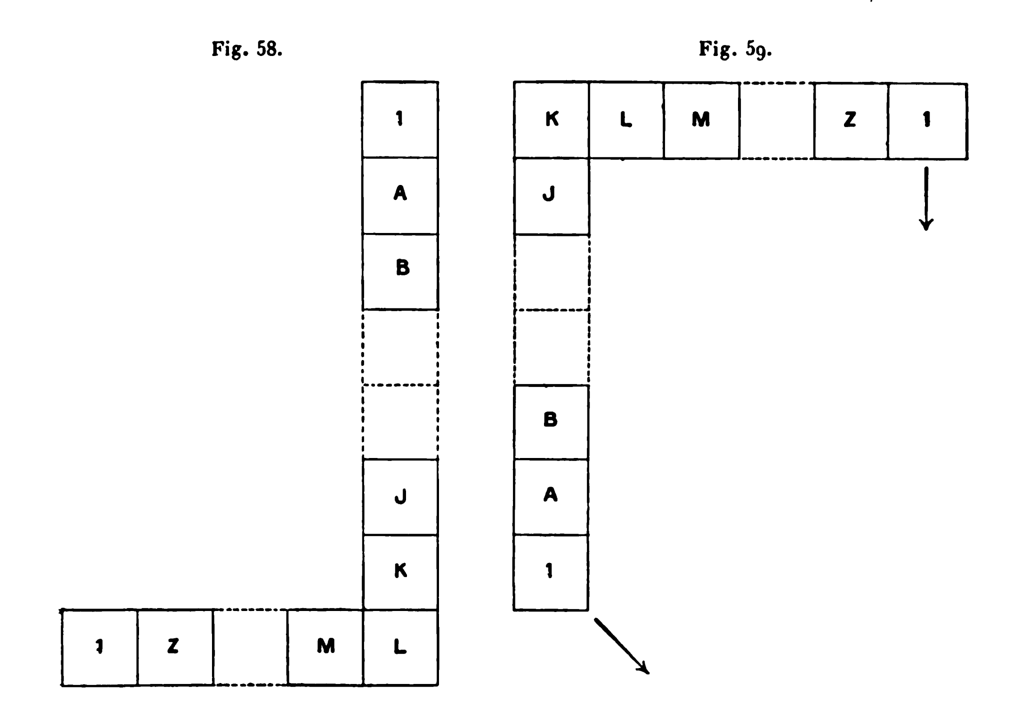
Théorème de l'angle droit.

que tout nombre contenu dans une case quelconque U d'un tableau de sommes est égal à la somme des nombres contenus dans les cases marquées 1, et pris une seule fois.

Si l'on remplace, à partir du bas, toutes les cases marquées

par les deux cases correspondantes de la loi de formation, on obtient la *fig.* 56, qui montre que le nombre contenu dans la case U est égal à la somme des nombres contenus dans les cases marquées 1, 2, ..., 6, 7, 1, multipliés respectivement par ces coefficients; on passera de même à la *fig.* 57. On peut aussi, en partant de la droite, remplacer les cases du haut par les cases qui correspondent à la loi de formation. Par induction, on en déduit le théorème suivant, qui s'applique dans toute l'étendue d'un tableau de sommes :

Fig. 58. Fig. 59.



Si l'on considère, dans le triangle de Pascal, un angle droit (*fig.* 58) formé avec les premières cases d'une ligne et les cases supérieures d'une colonne, de rangs quelconques; puis, si l'on élève d'un rang, en les déplaçant en même temps, d'un rang vers la gauche, toutes les cases du côté inférieur, et si l'on fait tourner ensuite l'angle obtenu d'un demi-tour autour de son sommet, on obtient l'angle de la *fig.* 59. Cela fait, si l'on pose

cet angle sur les cases d'un tableau de sommes, la somme des produits obtenus en multipliant le nombre de chaque case par le coefficient correspondant de l'angle est égale au terme du tableau qui se trouve dans la même colonne ↓ que le 1 supérieur de l'angle droit, et dans la même diagonale ↘ descendante que le 1 inférieur de l'angle.

Lorsque le côté vertical de l'angle se réduit à deux cases, on retrouve le théorème 1 (nº 75). Les autres théorèmes donnent lieu à des généralisations semblables à la précédente. Nous laissons au lecteur le soin d'étudier les propriétés des termes d'un tableau de sommes, dans ses rapports avec les coefficients du triangle de Pascal situés dans les parallèles à la diagonale ascendante ↗.

Lorsque l'on écrit le tableau des sommes et des différences dans la disposition du carré arithmétique (nº 53), les théorèmes qui précèdent prennent une forme plus symétrique. On peut, d'ailleurs, les démontrer directement sur une figure. Ainsi, on aperçoit tout de suite (*fig.* 60), que, dans tout tableau de sommes

Fig. 60.

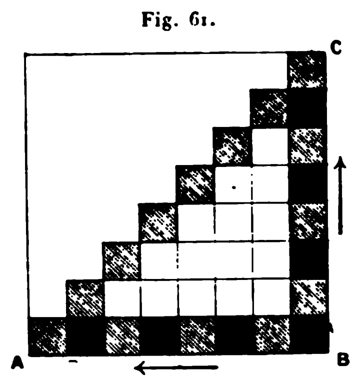
C_1 C_2 C_3

disposé comme le carré arithmétique, le terme contenu dans la case noire des *fig.* C_1, C_2, C_3 est égal à la somme des termes contenus respectivement dans les cases d'une diagonale ascendante, multipliés respectivement par les coefficients des développements $(1+x)^2$, de $(1+x)^3$ et de $(1+x)^4$.

En général, si l'on multiplie $(n+1)$ termes du Tableau (*fig.* 61) contenus dans les cases de la diagonale ↗ AC par les coefficients du développement de $(1+x)^n$, on trouve le terme contenu dans la case B. Si l'on multiplie $(n+1)$ termes contenus dans la ligne ← BA, respectivement par les coefficients de $(1-x)^n$, on obtient le terme C. Enfin, si l'on multiplie $(n+1)$ termes conte-

nus dans la colonne ↑BC, par les mêmes coefficients, on obtient le terme A.

Fig. 61.



Ces propriétés s'appliquent à l'échiquier triangulaire, au pentagone arithmétique et à l'hexagone, en supposant que ces tableaux sont prolongés indéfiniment dans tous les sens, par la même loi de formation.

PUISSANCES DES POLYNOMES.

79. **Puissances du trinôme et du quadrinôme.** — Si l'on fait le développement de $(a+b+c)^p$, en considérant $(a+b)$ comme une seule quantité, on a

$$\begin{aligned}(a+b+c)^p = (a+b)^p + C_p^1 (a+b)^{p-1} c + \ldots \\ + C_p^q (a+b)^{p-q} c^q + \ldots + c^p;\end{aligned}$$

en développant ensuite les binômes du second membre, nous obtiendrons le développement de la puissance du trinôme. D'abord, on voit que le nombre des termes, tous dissemblables, est, en commençant par la droite,

$$1+2+3+\ldots+(p+1) = \frac{(p+1)(p+2)}{1.2};$$

chaque terme sera de la forme $Ra^\alpha b^\beta c^\gamma$, en supposant que les nombres α, β, γ soient positifs ou nuls et aient p pour somme. On trouve ainsi, avec la convention $0! = 1$,

$$(a+b+c)^p = \Sigma \frac{p!}{\alpha!\,\beta!\,\gamma!} a^\alpha b^\beta c^\gamma.$$

De même, si l'on fait le développement de $(a+b+c+d)^p$,

en considérant $(a+b+c)$ comme une seule quantité, on trouve que le nombre des termes, après le développement des puissances du trinôme $(a+b+c)$, est

$$\frac{1.2}{1.2}+\frac{2.3}{1.2}+\frac{3.4}{1.2}+\ldots+\frac{(p+1)(p+2)}{1.2}=\frac{(p+1)(p+2)(p+3)}{1.2.3},$$

et l'on a

$$(a+b+c+d)^p=\Sigma\,\frac{p!}{\alpha!\,\beta!\,\gamma!\,\delta!}\,a^\alpha b^\beta c^\gamma d^\delta$$

pour toutes les valeurs entières, positives ou nulles de α, β, γ, δ, qui vérifient la relation

$$\alpha+\beta+\gamma+\delta=p.$$

Et ainsi de suite.

80. Puissances des polynômes. — On peut encore établir le théorème général de la manière suivante. Considérons le polynôme de q termes

$$a+b+c+\ldots+l,$$

et multiplions-le par lui-même, en écrivant les termes dans l'ordre ordinaire, c'est-à-dire en multipliant d'abord le multiplicande par a

$$aa+ba+ca+\ldots+la;$$

puis par b, puis par c, ..., par l; nous formons ainsi le carré du polynôme. Si nous ne nous servons pas d'exposants, et si nous ne faisons pas la réduction des termes semblables, les q^2 termes du produit représentent les B_q^2 arrangements complets des q lettres, prises deux à deux. En multipliant encore par le polynôme, sans faire de réduction, nous obtenons les B_q^3 arrangements complets des q lettres, prises trois à trois, et ainsi de suite jusqu'à B_q^p. Si l'on fait ensuite la réduction des termes semblables, on voit que le terme $a^\alpha b^\beta c^\gamma \ldots l^\lambda$, de degré p, aura pour coefficient le nombre des permutations avec répétition de p lettres dans lesquelles α sont égales à a, β à b, ..., λ à l; on a donc

$$(1)\qquad (a+b+c+\ldots+l)^p=\sum\frac{p!}{\alpha!\beta!\gamma!\ldots\lambda!}a^\alpha b^\beta c^\gamma\ldots l^\lambda.$$

Quant au nombre des termes du développement du second membre, il est égal au nombre des combinaisons complètes de q lettres, prises p à p, c'est-à-dire à

$$D_q^p=C_{p+q-1}^p=C_{p+q-1}^{q-1};$$

c'est, en effet, le nombre des mots de p lettres faits avec un alphabet de q lettres, chaque lettre pouvant être répétée jusqu'à p fois, mais de telle sorte que, dans chaque mot, les lettres soient rangées suivant l'ordre alphabétique.

Soit, par exemple, $p = 5$, on a

$$(\Sigma a)^5 = \Sigma a^5 + 5\Sigma a^4 b + 10\Sigma a^3 b^2 + 20\Sigma a^3 bc$$
$$+ 30\Sigma a^2 b^2 c + 60\Sigma a^2 bcd + 120\Sigma abcde.$$

On observera que les Σ du second membre de cette formule ont une signification bien différente de ceux qui se trouvent dans les formules qui précèdent : dans cette dernière formule, comme dans celles du n° 67, les Σ représentent des fonctions symétriques dont la théorie sera exposée plus loin. La détermination du nombre de ces Σ revient à trouver toutes les manières de former un nombre p par l'addition d'entiers positifs non croissants ; cette question rentre dans la théorie de la *partition des nombres*.

Exemple I. — Déterminer, pour les dix premières valeurs de p, le nombre des manières de former p par l'addition d'entiers positifs non croissants.

On forme le Tableau suivant (*fig.* 62) par la formule

$$N_p^q = N_{p-1}^{q-1} + N_{p-q}^q ;$$

Fig. 62.

p	1	2	3	4	5	6	7	8	9	10	N
1	1										1
2	1	1									2
3	1	1	1								3
4	1	2	1	1							5
5	1	2	2	1	1						7
6	1	3	3	2	1	1					11
7	1	3	4	3	2	1	1				15
8	1	4	5	5	3	2	1	1			22
9	1	4	7	6	5	3	2	1	1		30
10	1	5	8	9	7	5	3	2	1	1	42

Partition des nombres.

Ainsi, le nombre des manières de former $p = 7$, par l'addition de nombres

non croissants, est égal à la somme des nombres de la septième ligne

$$1,\ 3,\ 4,\ 3,\ 2,\ 1,\ 1$$

qui correspondent aux nombres de solutions qui commencent respectivement par

$$7,\ 6,\ 5,\ 4,\ 3,\ 2,\ 1.$$

Exemple II. — Calculer les coefficients du carré de

$$1 + x + x^2 + \ldots + x^n.$$

Exemple III. — Calculer les coefficients des dix premières puissances du trinôme $(1 + x + x^2)$.

Exemple IV. — Dans le développement du carré de

$$1 + x + 2x^2 + \ldots + px^p,$$

le coefficient de x^q, pour $q < p$, est égal à

$$\frac{q^3 + 11q}{6}.$$

Exemple V. — Le nombre des manières dont on peut amener le point n avec p dés à jouer est le coefficient de x^n dans le développement de la puissance

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^p.$$

Exemple VI. — Le produit

$$3(x^3 + y^3 + z^3)^2[(y + z)^3 + (z + x)^3 + (x + y)^3]$$

est la somme des cubes des polynômes

$$2x^3 - y^3 - z^3 + 3x(y^2 + z^2),$$
$$2y^3 - z^3 - x^3 + 3y(z^2 + x^2),$$
$$2z^3 - x^3 - y^3 + 3z(x^2 + y^2).$$

81. Arrangements figurés. — Nous donnerons une démonstration de la formule (1) du numéro précédent, qui repose sur les arrangements figurés.

Considérons un échiquier formé de p lignes horizontales et de a colonnes verticales; déterminons le nombre des manières de placer α pions sur des cases différentes de l'échiquier, et de telle sorte qu'il n'y en ait pas deux sur une même ligne. On observera que ce nombre est nul pour $\alpha > p$; nous supposerons donc $\alpha \leqq p$.

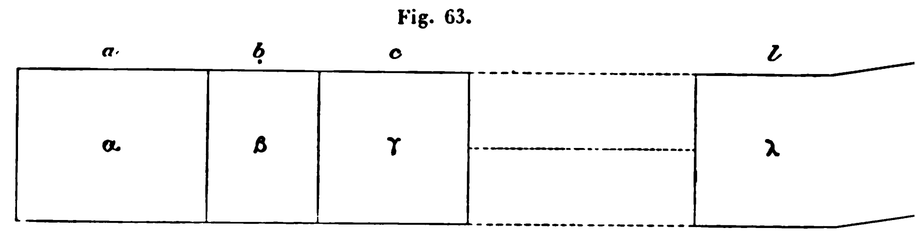
Il faut d'abord choisir α lignes, parmi les p lignes données, ce qui fait C_p^α combinaisons simples ; puis, sur chacune des lignes choisies, il y a a places ; il en résulte a^α dispositions différentes pour une même combinaison de α lignes ; donc le nombre cherché est $C_p^\alpha a^\alpha$, ou, en nous servant de la notation des factorielles

$$\frac{p!}{\alpha!(p-\alpha)!}\,a^\alpha.$$

En particulier, pour $\alpha = p$, on obtient la figuration des arrangements complets B_a^p de a objets, pris p à p, qui sont en nombre a^p.

Cela posé, considérons un échiquier de hauteur p et de longueur $(a+b+c+\ldots+l)$; on peut imaginer que cet échiquier est formé par l'accolement d'échiquiers de même hauteur p et dont les longueurs sont respectivement représentées par $a, b, c, \ldots, l$.

Fig. 63.



Arrangements figurés.

Le nombre de manières de placer p pions sur des cases différentes de l'échiquier total, de telle sorte qu'il n'y en ait pas deux sur une même ligne, est égal, d'après ce qui précède, à

$$(a+b+c+\ldots+l)^p.$$

Mais, pour une disposition quelconque, il existe, dans chacun des échiquiers partiels, des pions en nombres $\alpha, \beta, \gamma, \ldots, \lambda$, nuls ou positifs, qui vérifient de toutes les manières possibles la relation

$$\alpha+\beta+\gamma+\ldots+\lambda = p.$$

Prenons des valeurs déterminées de $\alpha, \beta, \gamma, \ldots, \lambda$ qui vérifient cette relation, et cherchons le nombre des dispositions correspon-

dantes des p pions sur les cases de l'échiquier total. Ce nombre est évidemment égal au produit des nombres des dispositions de α pions sur les p lignes du premier échiquier partiel, de β pions sur $(p-\alpha)$ lignes du second, de γ pions sur $(p-\alpha-\beta)$ lignes du troisième, et ainsi de suite; on trouve ainsi

$$\frac{p!}{\alpha!(p-\alpha)!}\,a^\alpha \times \frac{(p-\alpha)!}{\beta!(p-\alpha-\beta)!}\,b^\beta \times \frac{(p-\alpha-\beta)!}{\gamma!(p-\alpha-\beta-\gamma)!}\,c^\gamma \times \ldots,$$

ou, après réductions,

$$\frac{p!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!}\,a^\alpha b^\beta c^\gamma \ldots l^\lambda.$$

En faisant la somme de ces nombres, pour toutes les solutions de l'équation de condition, on obtient la formule (1) du n° 80. Avec la notation des arrangements complets, cette formule peut s'écrire

$$\mathrm{B}^p_{a+b+c+\ldots+l} = \sum \frac{p!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!}\,\mathrm{B}^\alpha_a \mathrm{B}^\beta_b \mathrm{B}^\gamma_c \ldots \mathrm{B}^\lambda_l.$$

Mais, au lieu de traiter le problème par la seule condition qu'il n'y ait pas deux pions sur une même ligne, on peut ajouter cette condition qu'il n'y en ait pas deux sur une même colonne; alors les *Arrangements complets figurés* se transforment en *Arrangements simples figurés,* et l'on a la formule

$$\mathrm{A}^p_{a+b+c+\ldots+l} = \sum \frac{p!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!}\,\mathrm{A}^\alpha_a \mathrm{A}^\beta_b \mathrm{A}^\gamma_c \ldots \mathrm{A}^\lambda_l;$$

Cette formule donne l'extension aux polynômes de la formule du binôme de Vandermonde.

Remarque. — Au lieu de supposer que les lignes de chaque échiquier partiel contiennent le même nombre de cases, on peut supposer que les p lignes du premier contiennent respectivement $a_1, a_2, \ldots, a_p$ cases; que les p lignes du second contiennent $b_1, b_2, \ldots, b_p$ cases, et ainsi de suite. On peut, de plus, admettre que chaque case de l'échiquier peut recevoir jusqu'à n pions, que chaque ligne peut contenir respectivement jusqu'à $n_1, n_2, \ldots, n_p$ pions; en outre, on peut encore faire des conventions pour chacune des colonnes de l'échiquier.

En traitant alors ce problème général de la disposition des pions, en l'étendant aux échiquiers cubiques, et au delà, on obtient des formules qui donnent, comme cas très particuliers, les formules les plus générales de WARING, dans la théorie des *Fonctions symétriques*, et celles de WRONSKI, dans la théorie des *Facultés arithmétiques* et dans sa *Loi suprême des différences*.

LIVRE II.

LES NOMBRES RATIONNELS.

CHAPITRE IX.

LES NOMBRES FRACTIONNAIRES.

82. Les nombres fractionnaires. — Nous admettons que l'unité peut être divisée en n parties égales, que l'on désigne par $\frac{1}{n}$; ce postulatum correspond à celui d'Euclide, puisque celui-ci revient à la division d'une longueur en parties égales. Mais on peut se passer de ce postulatum, si l'on veut se reporter à l'Introduction de cet Ouvrage.

Définitions d'une fraction $\frac{p}{q}$ et de ses deux termes. *Numérateur* et *Dénominateur*.

Addition et soustraction des fractions de même dénominateur.

Multiplication et division d'une fraction par un entier.

On ne change pas la valeur d'une fraction en multipliant ses deux termes par un entier.

Réduction des fractions au même dénominateur ([1]).

Addition et Soustraction des fractions. — Simplification des résultats, lorsque l'on aperçoit un facteur commun aux deux termes.

([1]) Les théories du plus petit dénominateur commun et du plus grand commun diviseur sont reportées à la divisibilité arithmétique. La théorie des fractions décimales périodiques est reportée à celle des congruences binômes.

Multiplication des fractions. — Le résultat est indépendant de l'ordre des multiplications. — Puissances des fractions.

Division des fractions. — Fractions de fractions.

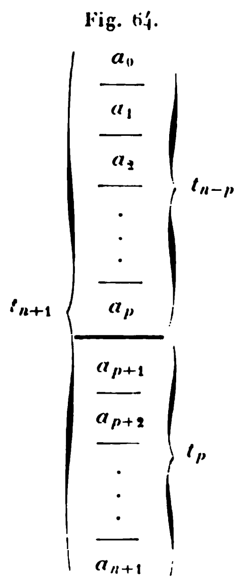
En général, les règles et les théorèmes sur les quatre opérations fondamentales des fractions à termes entiers et positifs s'appliquent aux expressions fractionnaires dont les termes sont des fractions.

Exemple I. — On exprime le nombre 100 par une somme de nombres fractionnaires ne contenant qu'une seule fois les neuf chiffres significatifs par l'égalité

$$100 = 97 + \frac{5+3}{8} + \frac{6}{4} + \frac{1}{2}.$$

Exemple II. — *Les fractions étagées.* — C'est une suite de nombres $a_0, a_1, a_2, \ldots, a_{n+1}$, qui sont disposés verticalement et séparés successivement par $(n+1)$ *barres* de fractions. Cette notation ne saurait être em-

Fig. 64.



Les fractions étagées.

ployée en Arithmétique, sans l'adjonction de parenthèses, car elle n'aurait pas de sens précis. Mais il y a lieu de déterminer le nombre des résultats que l'on peut obtenir en laissant à ce symbole sa plus large signification.

Désignons par $(n+1)$ le nombre des barres de fraction, par t_{n+1} le nombre d'interprétations correspondantes; supposons que la fraction étagée de $(n+1)$ barres se compose du quotient de deux autres contenant respectivement p et $(n-p)$ barres; le nombre des interprétations différentes est, dans ce cas, égal au produit de t_p par t_{n-p}. Par conséquent, si l'on suppose p successivement égal à la suite des entiers 0, 1, 2, ..., n, on a la loi de récurrence

$$t_{n+1} = t_0 t_n + t_1 t_{n-1} + t_2 t_{n-2} + \ldots + t_{n-1} t_1 + t_n t_0.$$

D'ailleurs, pour les premières valeurs de n,

$$t_0 = 1, \quad t_1 = 1, \quad t_2 = 2, \quad t_3 = 5, \quad \ldots;$$

par conséquent, en se reportant à l'*Exemple IV* du n° 54, on en déduit

$$t_n = \frac{1}{n+1} C_{2n}^n.$$

83. Les nombres inverses ou réciproques. — Deux nombres fractionnaires sont dits *inverses ou réciproques,* lorsque leur produit est 1. Ainsi a et $\frac{1}{a}$ sont des nombres inverses, pour toute valeur entière de a, positive ou négative, et puisque la série des nombres entiers est illimitée, il en est de même de la série de leurs inverses. On peut donc considérer des suites indéfinies de fractions qui s'approchent de zéro autant qu'on veut, sans que ces fractions soient constamment nulles. De là, la notion d'*infiniment petit* qui se déduit de celle du *nombre infini,* de même que la division est l'inverse de la multiplication.

Les *Tables des nombres inverses,* ou réciproques, sont très utiles pour la simplification des calculs; la Table la plus étendue, celle de Oakes, publiée à Londres en 1865, donne les premières décimales des inverses des nombres entiers jusqu'à 100000; au moyen de Tables proportionnelles, on peut encore obtenir facilement les sept premières décimales des inverses de tous les entiers jusqu'à 10000000. L'emploi simultané de cette Table et d'un procédé rapide de multiplication, comme celui de la Table des quarts de carrés, permet de remplacer, dans les calculs approchés, la division $(a:b)$ par la multiplication de a par l'inverse de b (n° 25).

84. Les fractions algébriques. — Les règles énoncées dans les numéros précédents s'appliquent aux fractions algébriques. Par

suite, les opérations algébriques de l'addition, de la soustraction et de la multiplication, s'appliquent aux polynômes dans lesquels les coefficients et les variables sont des nombres fractionnaires, positifs ou négatifs. Il en est de même des théorèmes sur la divisibilité par $(x - a)$, et sur l'identité des polynômes (nos **72** et **73**).

Division des monômes. — Règle des signes. — Règle des exposants.

Exposant zéro. — Exposants entiers négatifs. — Les théorèmes représentés par les trois formules

$$a^p \times a^q = a^{p+q},$$
$$a^p : a^q = a^{p-q},$$
$$(a^p)^q = a^{pq}$$

s'appliquent à toutes les valeurs entières, positives, nulles ou négatives des exposants p et q.

Exemple I. — Si l'on ajoute terme à terme des fractions dont les dénominateurs ont le même signe, on obtient une fraction intermédiaire, c'est-à-dire comprise entre la plus petite et la plus grande d'entre elles. — Cas de l'égalité des fractions.

Les anciens mathématiciens de l'Inde, de l'Égypte et de la Grèce, ont souvent employé le procédé dit de *médiation*, qui consiste à remplacer deux fractions

$$\frac{c}{d} \quad \text{et} \quad \frac{a}{b},$$

par leur médiante $\frac{a+c}{b+d}$, comprise entre les deux premières, pourvu que b et d soient positifs. Ainsi, par exemple, les deux nombres

$$\frac{22}{7} \quad \text{et} \quad \frac{333}{106},$$

donnés par ARCHIMÈDE et par les géomètres indiens, qui représentent par excès et par défaut le rapport de la circonférence au diamètre, conduisent, par le procédé de médiation, au rapport $\frac{355}{113}$ donné par METIUS.

Exemple II. — Vérifier la formule

$$\left(\frac{a-b}{c} + \frac{b-c}{a} + \frac{c-a}{b}\right)\left(\frac{c}{a-b} + \frac{a}{b-c} + \frac{b}{c-a}\right) = 9,$$

en supposant $a + b + c = 0$.

85. Les progressions harmoniques. — On dit que des nombres forment une *progression harmonique* lorsque leurs inverses sont en progression arithmétique. Nous représenterons cette progression par

$$\frac{1}{a},\ \frac{1}{b},\ \frac{1}{c},\ \ldots,\ \frac{1}{h},\ \frac{1}{k},\ \frac{1}{l},$$

a, b, c, ..., h, k, l, désignant des termes en progression arithmétique de raison r; d'ailleurs, nous supposerons, dans ce qui suit, qu'il n'y a aucun dénominateur nul.

En particulier, les inverses des nombres entiers forment la *série harmonique*

$$\frac{1}{1},\ \Big|\ \frac{1}{2},\ \Big|\ \frac{1}{3},\ \frac{1}{4},\ \Big|\ \frac{1}{5},\ \frac{1}{6},\ \frac{1}{7},\ \frac{1}{8},\ \Big|\ \frac{1}{9},\ \ldots,\ \frac{1}{16},\ \Big|\ \ldots.$$

En partageant cette série en groupes renfermant successivement 1, 1, 2, 4, 8, ..., 2^n termes, on voit que chacun de ceux-ci est plus grand que le dernier de son groupe, et que la somme des termes de chaque groupe est plus grande que $\frac{1}{2}$. La somme des termes de la série augmente indéfiniment ; la série est dite *divergente*.

Plus généralement, la somme des termes d'une progression harmonique indéfinie est divergente. En effet, pour un terme quelconque, on a

$$\frac{1}{a+nr} = \frac{1}{r}\,\frac{1}{\frac{a}{r}+n};$$

en désignant par p l'entier plus grand que $\left(n+\frac{a}{r}\right)$, les termes de la progression sont respectivement, à partir de ce terme, plus petits que le quotient par r des termes

$$\frac{1}{p},\ \frac{1}{p+1},\ \frac{1}{p+2},\ \ldots$$

de la série harmonique.

On ne connaît pas de formule simple pour exprimer la somme des termes d'une progression harmonique.

Exemple I. — On a l'identité

$$1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots,+\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}.$$

On la démontre immédiatement en retranchant des termes de rang pair de la somme des $2n$ premiers termes de la série harmonique la somme des n premiers termes de celle-ci (CATALAN).

Exemple II. — On a l'identité suivante, due à DIRICHLET,

$$\left(1-\frac{1}{2}-\frac{1}{4}\right)+\left(\frac{1}{3}-\frac{1}{6}-\frac{1}{8}\right)+\ldots+\left(\frac{1}{2n-1}-\frac{1}{4n-2}-\frac{1}{4n}\right)$$
$$=\frac{1}{2}\left(1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots+\frac{1}{2n-1}-\frac{1}{2n}\right).$$

Cette formule se démontre immédiatement, en réunissant chaque terme positif de la parenthèse avec le terme négatif qui le suit. Ainsi

$$\frac{1}{2n-1}-\frac{1}{4n-2}-\frac{1}{4n}=\frac{1}{2}\left(\frac{1}{2n-1}-\frac{1}{2n}\right).$$

86. Sommation des inverses des factorielles. — Si l'on pose

$$H_2=\frac{1}{ab}+\frac{1}{bc}+\frac{1}{cd}+\ldots+\frac{1}{kl},$$
$$H_3=\frac{1}{abc}+\frac{1}{bcd}+\frac{1}{cde}+\ldots+\frac{1}{hkl},$$
$$H_4=\frac{1}{abcd}+\frac{1}{bcde}+\frac{1}{cdef}+\ldots+\frac{1}{ghkl},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

et si l'on part des égalités

$$\frac{r}{ab}=\frac{1}{a}-\frac{1}{b},$$
$$\frac{2r}{abc}=\frac{1}{ab}-\frac{1}{bc},$$
$$\frac{3r}{abcd}=\frac{1}{abc}-\frac{1}{bcd},$$
$$\ldots\ldots\ldots\ldots,$$

on trouve, en sommant les égalités obtenues, comme au n° 37,

$$r.H_2=\frac{1}{a}-\frac{1}{l},$$
$$2r.H_3=\frac{1}{ab}-\frac{1}{kl},$$
$$3r.H_4=\frac{1}{abc}-\frac{1}{hkl},$$
$$\ldots\ldots\ldots\ldots$$

En particulier, si l'on considère la série harmonique, on a les formules de LEIBNIZ et de STIRLING

$$\frac{1}{1.2}+\frac{1}{2.3}+\frac{1}{3.4}+\frac{1}{4.5}+\ldots+\frac{1}{n(n+1)}=1-\frac{1}{n+1},$$

$$\frac{1}{1.2.3}+\frac{1}{2.3.4}+\ldots+\frac{1}{n(n+1)(n+2)}=\frac{1}{2}\left[\frac{1}{1.2}-\frac{1}{(n+1)(n+2)}\right],$$

$$\frac{1}{1.2.3.4}+\ldots+\frac{1}{n(n+1)(n+2)(n+3)}=\frac{1}{3}\left[\frac{1}{1.2.3}-\frac{1}{(n+1)(n+2)(n+3)}\right],$$

. . . .

On peut, d'ailleurs, vérifier *a posteriori* la formule suivante, qui les renferme toutes :

$$\sum_{x=1}^{x=n}\frac{1}{x(x+1)\ldots(x+p)}=\frac{1}{p}\left[\frac{1}{p!}-\frac{1}{(n+1)\ldots(n+p)}\right].$$

Lorsque l'entier n augmente indéfiniment, cette somme a pour limite

$$\frac{1}{p.p!}.$$

Exemple I. — Si le premier terme d'une progression arithmétique est $a=1$, comme dans les progressions donnant naissance aux nombres polygonaux (n° 36), on a

$$a+2ab+3abc+\ldots+(n-1)abc\ldots k=\frac{1}{r}[abc\,..kl-1],$$

$$\frac{1}{ab}+\frac{2}{abc}+\frac{3}{abcd}+\ldots+\frac{n-1}{abc\ldots l}=\frac{1}{r}\left[1-\frac{1}{abc\ldots l}\right].$$

En particulier,

$$1.1!+2.2!+3.3!+\ldots+n.n!=(n+1)!-1,$$

$$\frac{1}{2!}+\frac{2}{3!}+\frac{3}{4!}+\ldots+\frac{n}{(n+1)!}=1-\frac{1}{(n+1)!}.$$

Exemple II. — Si l'on pose

$$\frac{e_n}{n!}=1+\frac{1}{1!}+\frac{1}{2!}+\ldots+\frac{1}{n!},$$

on a les formules

$$e_{n+1}=(n+1)\,e_n+1,$$
$$e_{n+1}=(n+2)\,e_n-ne_{n-1}.$$

Exemple III. — Si deux progressions arithmétiques

$$a,\ b,\ c,\ \ldots,\ k,\ l,$$
$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \varkappa,\ \lambda,$$

ont la même raison r et le même nombre de termes, on a la formule

$$\frac{a}{\alpha\beta}+\frac{ab}{\alpha\beta\gamma}+\ldots+\frac{abc\ldots k}{\alpha\beta\gamma\ldots\varkappa\lambda}=\frac{1}{r}\left[\frac{a}{\alpha}-\frac{abc\ldots l}{\alpha\beta\gamma\ldots\lambda}\right].$$

En mettant $\frac{1}{\alpha}$ en facteur, les fractions du premier membre ont, dans les deux termes, le même nombre de facteurs.

87. Triangle harmonique de Leibniz. — Si l'on pose

$$u_n=\frac{1}{n},$$

on a, avec les notations du calcul des différences,

$$\Delta u_n=\frac{1}{n+1}-\frac{1}{n}=-\frac{1}{n(n+1)},$$
$$\Delta^2 u_n=\frac{1}{(n+1)(n+2)}-\frac{1}{n(n+1)}=\frac{1.2}{n(n+1)(n+2)},$$

et, en général,

$$\Delta^p u_n=\frac{(-1)^p p!}{n(n+1)\ldots(n+p)}.$$

Par conséquent, le Tableau des différences de la fonction u_n représente les inverses des factorielles successives multipliées, dans chaque colonne, par un même nombre, ou encore les inverses des termes du triangle de Pascal, divisés, dans chaque colonne, par un même nombre; ce Tableau diffère peu du *Triangle harmonique* de Leibniz. En appliquant à ce Tableau deux des formules fondamentales du calcul des différences (n°s 75 et 76), on a ainsi

$$\frac{p!}{n(n+1)\ldots(n+p)}=\frac{1}{n}-\frac{C_p^1}{n+1}+\frac{C_p^2}{n+2}-\ldots+\frac{(-1)^p}{n+p};$$
$$\frac{1}{n+p}=\frac{1}{n}-\frac{p}{n(n+1)}+\frac{p(p-1)}{n(n+1)(n+2)}-\ldots+\frac{(-1)^p p!}{n(n+1)\ldots(n+p)}.$$

Ces formules subsistent en remplaçant le nombre entier n par un nombre fractionnaire quelconque x.

Exemple I. — Si la progression arithmétique de raison r a $(p+1)$ termes, on trouve

$$\frac{p!\,r^p}{abc\ldots l} = \frac{1}{a} - \frac{C_p^1}{b} + \frac{C_p^2}{c} - \ldots + \frac{(-1)^p}{l},$$

$$\frac{1}{l} = \frac{1}{a} - \frac{rA_p^1}{ab} + \frac{r^2A_p^2}{abc} - \ldots + \frac{(-r)^pA_p^p}{abc\ldots l},$$

en désignant respectivement par les lettres C et A les combinaisons et les arrangements simples.

Exemple II. — La fraction

$$\frac{x(x+2)(x+4)\ldots(x+2p-2)}{(x+1)(x+3)(x+5)\ldots(x+2p-1)}$$

est égale au développement de

$$1 - C_p^1\frac{1}{x+1} + C_p^2\frac{1.3}{(x+1)(x+3)} - C_p^3\frac{1.3.5}{(x+1)(x+3)(x+5)} + \ldots.$$

Exemple III. — La fraction

$$\frac{1.3.5\ldots(2p-1)}{(x+1)(x+3)\ldots(x+2p-1)}$$

est égale au développement de l'expression

$$1 - C_p^1\frac{x}{x+1} + C_p^2\frac{x(x+2)}{(x+1)(x+3)} - C_p^3\frac{x(x+2)(x+4)}{(x+1)(x+3)(x+5)} + \ldots.$$

Exemple IV. — La fraction

$$\frac{2.4.6\ldots(2p)}{(x+2)(x+4)\ldots(x+2p)}$$

est égale au développement de

$$1 - C_p^1\frac{x}{x+2} + C_p^2\frac{x}{x+4} - C_p^3\frac{x}{x+6} + \ldots.$$

Exemple V. — Si $n > 2$ est un entier pair, on a

$$n = 1 + \frac{n-1}{n-2} + \frac{(n-1)(n-3)}{(n-2)(n-4)} + \ldots$$
$$+ \frac{(n-1)\ldots9.7.5}{(n-2)\ldots8.6.4} + 2\,\frac{(n-1)\ldots7.5.3}{(n-2)\ldots6.4.2},$$

et si n est un entier impair, on a

$$n = 1 + \frac{n-1}{n-2} + \frac{(n-1)(n-3)}{(n-2)(n-4)} + \ldots + \frac{(n-1)\ldots 6.4.2}{(n-2)\ldots 5.3.1}.$$

Exemple VI. — Quels que soient les nombres $a, b, c, \ldots, k, l$, on a l'identité

$$1 + \frac{1}{a} + \frac{a+1}{ab} + \frac{(a+1)(b+1)}{abc} + \ldots + \frac{(a+1)(b+1)\ldots(k+1)}{abc\ldots kl}$$
$$= \frac{(a+1)(b+1)\ldots(l+1)}{abc\ldots kl}.$$

88. Les progressions géométriques. — Une progression géométrique est une suite de nombres tels que chacun d'eux est égal au précédent multiplié par un nombre constant q que l'on appelle *raison* de la progression. Nous désignerons par

$$\div\div\, a, b, c, \ldots, h, k, l$$

les n termes de la progression, par P et par S le produit et la somme des termes. On a les propriétés suivantes :

I. Le quotient de deux termes de la progression est une puissance de la raison dont l'exposant égale la différence des rangs des deux termes.

II. Si l'on multiplie ou si l'on divise terme à terme deux progressions géométriques, on obtient une progression géométrique dont la raison égale le produit ou le quotient des raisons des progressions données.

III. Le produit de deux termes équidistants des extrêmes égale le produit des extrêmes.

IV. Le carré du produit des termes d'une progression géométrique égale le produit des extrêmes élevé à une puissance dont l'exposant est égal au nombre des termes.

On a donc

$$l = aq^{n-1}, \qquad P^2 = (al)^n, \qquad P = a^n q^{\frac{n(n-1)}{2}}.$$

89. Somme des termes d'une progression géométrique. — Pour $q = 1$, on a $S = na$, et pour $q \gtrless 1$,

$$S = \frac{lq - a}{q - 1},$$

ou encore

$$S = a\frac{q^n - 1}{q - 1}.$$

Les puissances successives des nombres plus grands que 1 vont en croissant et peuvent dépasser un nombre donné, quelque grand qu'il soit.

Les puissances successives des nombres positifs plus petits que 1 vont en décroissant et peuvent devenir plus petites qu'un nombre donné, si petit qu'il soit.

La progression est croissante ou décroissante selon que la raison, supposée positive, est plus grande ou plus petite que 1. Elle est alternée, lorsque la raison est un nombre négatif.

La somme des termes d'une progression géométrique indéfinie dont la raison est un nombre plus petit que 1, en valeur absolue, a pour limite

$$\frac{a}{1 - q}.$$

Exemple I. — Un tonneau contient a litres de vin. On en tire un litre que l'on remplace par un litre d'eau; puis on tire un second litre du mélange, que l'on remplace par un litre d'eau, et ainsi de suite. Quelle est la quantité de vin que contiendra le tonneau après n opérations?

Réponse

$$\frac{(a - 1)^n}{a^{n-1}}.$$

Exemple II. — Une femme porte des œufs au marché, elle en vend à une première personne la moitié, plus la moitié d'un œuf; à une seconde personne, la moitié de ce qui lui reste, plus la moitié d'un œuf. Après n opérations de ce genre, elle a tout vendu. Combien la marchande avait-elle d'œufs en arrivant au marché?

A la dernière personne, la marchande a vendu un œuf; à l'avant-dernière, deux œufs; à la précédente quatre, et ainsi en remontant. Elle en avait donc en tout $2^n - 1$.

Exemple III. — Des joueurs en nombre n, et en ordre donné, conviennent que le perdant doublera l'argent des $(n - 1)$ autres. Ils perdent chacun une partie, dans l'ordre donné et, à la fin, ils ont chacun la même somme a. Combien chacun avait-il au commencement?

Le problème se résout en établissant la situation de chaque joueur après la $(n - 1)^{\text{ième}}$ partie, puis après la $(n - 2)^{\text{ième}}$ partie, et ainsi de suite, en remontant.

On trouve

$$\frac{1+2^{n-1}n}{2^n}a,\quad \frac{1+2^{n-2}n}{2^n}a,\quad \ldots,\quad \frac{1+n}{2^n}a.$$

Exemple IV. — Des joueurs en nombre n et en ordre donné jouent de la manière suivante. Le premier joue avec le deuxième et perd la $q^{\text{ième}}$ partie de ce qu'il a, le deuxième joue avec le troisième et perd la $q^{\text{ième}}$ partie de ce qu'il possède à ce moment, et ainsi de suite. Enfin le dernier joue avec le premier et perd la $q^{\text{ième}}$ partie de ce qu'il possède alors. A la fin du jeu, les joueurs possèdent la même somme a; quelle somme chacun d'eux avait-il au début du tournoi?

Exemple V. — Si l'on désigne par S_n et S_{n-1} la somme des n et des $(n-1)$ premiers termes d'une progression géométrique de raison q, la somme des produits deux à deux des n termes de la progression géométrique a pour expression

$$\frac{q}{q+1}S_nS_{n-1}.$$

Exemple VI. — On multiplie respectivement les n termes d'une progression arithmétique de raison r,

$$\div\, a, b, c, \ldots, h, k, l,$$

par les n premiers termes d'une progression géométrique de raison q,

$$\div\!\div\, \alpha, \beta, \gamma, \ldots, \eta, \varkappa, \lambda;$$

trouver la somme

$$a\alpha + b\beta + c\gamma + \ldots + i\lambda.$$

Exemple VII. — Si l'on désigne par u_n la somme des termes de rang n de deux progressions géométriques, ayant pour raisons q et q', on a la formule de récurrence

$$u_{n+2} = (q+q')u_{n+1} - qq'u_n.$$

Exemple VIII. — L'expression

$$(1+x+x^2+\ldots+x^n)^2 - x^n$$

est le produit des deux facteurs

$$1+x+x^2+\ldots+x^{n+1}$$

et

$$1+x+x^2+\ldots+x^{n-1}.$$

Exemple IX. — On a

$$(1+x)(1+x^2)(1+x^4)\ldots(1+x^{2^n}) = 1+x+x^2+x^3+\ldots+x^{2^{n+1}-1};$$

plus généralement, si l'on pose

$$f_p = 1 + x^p + x^{2p} + \ldots + x^{(p-1)p},$$

on a l'identité

$$f_1 f_2 \ldots f_p = 1 + x + x^2 + x^3 + \ldots + x^{p^n-1}.$$

Exemple X. — La somme de toutes les fractions de la forme $\frac{1}{(p+1)^{q+1}}$ a pour limite 1, lorsque l'on donne à p et q toutes les valeurs entières et positives (GOLDBACH). — En effet, il faut faire la somme des fractions

$$\begin{array}{lllll} \frac{1}{2^2}, & \frac{1}{2^3}, & \frac{1}{2^4}, & \frac{1}{2^5}, & \ldots, \\ \frac{1}{3^2}, & \frac{1}{3^3}, & \frac{1}{3^4}, & \frac{1}{3^5}, & \ldots, \\ \frac{1}{4^2}, & \frac{1}{4^3}, & \frac{1}{4^4}, & \frac{1}{4^5}, & \ldots, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Mais la limite de la somme des termes d'une ligne quelconque

$$\frac{1}{p^2}, \ \frac{1}{p^3}, \ \frac{1}{p^4}, \ \frac{1}{p^5}, \ \ldots, \ \text{est} \ \frac{1}{(p-1)p};$$

la somme des termes du tableau a donc pour limite (n° 86)

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \ldots + \frac{1}{(p-1)p} + \ldots = 1.$$

90. Propriétés des polynômes ordonnés. — Nous allons démontrer la proposition suivante : *Étant donné un polynôme $f(x)$, ne renfermant pas de terme constant, on peut trouver un nombre positif h tel que, pour toute valeur de x comprise entre $-h$ et $+h$, la valeur de $f(x)$ soit comprise entre $-k$ et $+k$, si k est un nombre positif donné, aussi petit qu'on voudra.* — En effet, soit

$$f(x) = a_1 x + a_2 x^2 + \ldots + a_n x^n;$$

soit ρ la valeur absolue de x, R la valeur correspondante de $f(x)$ et A la plus grande des valeurs absolues des coefficients du polynôme ; on a évidemment

$$R \overline{\gtrless} A(\rho + \rho^2 + \ldots + \rho^n),$$

ou

$$R \overline{\gtrless} \frac{A(\rho - \rho^{n+1})}{1-\rho},$$

et *a fortiori*, en supposant $\rho < 1$,

$$R < \frac{A\rho}{1-\rho};$$

d'ailleurs, de l'inégalité

$$\frac{A\rho}{1-\rho} < k,$$

on tire

$$\rho < \frac{k}{A+k}.$$

Si l'on désigne par h le second membre de l'inégalité précédente, on en déduit que le polynôme $f(x)$ est toujours compris entre $-k$ et $+k$, lorsque la valeur de x est comprise entre $-h$ et $+h$.

On a encore la proposition suivante : *Lorsqu'un polynôme est ordonné suivant les exposants croissants de x, on peut trouver un nombre positif h tel que, pour toute valeur de x comprise entre $-h$ et $+h$, le polynôme $f(x)$ ait le signe de son premier terme et en diffère d'aussi peu que l'on voudra.* — En effet, soit

$$f(x) = a_p x^p + a_{p+1} x^{p+1} + \ldots + a_n x^n$$

le polynôme donné; on a

$$\frac{f(x)}{a_p x^p} = 1 + \varphi(x),$$

et il suffit de déterminer h de telle sorte que le polynôme $\varphi(x)$ soit, en valeur absolue, plus petit qu'un nombre positif donné k.

Les deux théorèmes qui précèdent s'appliquent pour les exposants croissants; les deux qui suivent, pour les exposants décroissants : *Lorsqu'un polynôme est ordonné suivant les exposants décroissants, on peut trouver un nombre positif λ tel que, pour toute valeur de x dont la valeur absolue surpasse λ, le polynôme ait le signe de son premier terme.* — Soit, en effet,

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n;$$

si l'on remplace x par y^{-1}, on a

$$\frac{f(x)}{a_0 x^n} = 1 + \varphi(y)$$

$\varphi(y)$ désignant un polynôme ordonné suivant les exposants croissants de y et n'ayant pas de terme constant. On peut donc trouver un nombre positif h tel que pour toute valeur de y comprise entre $-h$ et $+h$, la valeur absolue du polynôme soit plus petite qu'un nombre positif donné k; par suite, si l'on pose $\lambda = h^{-1}$, lorsque la valeur absolue de x est plus grande que λ, le rapport du polynôme à son premier terme est compris entre $(1-k)$ et $(1+k)$.

Ainsi, lorsque la valeur absolue de x devient plus grande qu'un nombre aussi grand qu'on veut, le rapport du polynôme à son premier terme a pour limite 1. Plus généralement, lorsque x croît au delà de toute limite, le rapport de deux polynômes de même degré s'approche autant qu'on veut du rapport des coefficients des deux premiers termes.

Lorsqu'un polynôme est ordonné suivant les exposants décroissants, on peut trouver un nombre positif μ, *tel que la valeur absolue du polynôme* $f(x)$ *soit plus grande qu'un nombre positif* L, *donné aussi grand qu'on voudra.* — En effet, soit ρ la valeur absolue de x, R la valeur absolue de $f(x)$, et $r_0, r_1, \ldots, r_n$ les valeurs absolues des coefficients de $f(x)$. Puisque la valeur absolue de la somme de deux nombres est plus grande que la différence des valeurs absolues, on a, en considérant $f(x)$ comme la somme de son premier terme et de tous les autres

$$R > r_0\rho^n - (r_1\rho^{n-1} + \ldots + r_n);$$

si l'on pose $R > L$, c'est-à-dire

$$r_0\rho^n - (r_1\rho^{n-1} + r_2\rho^{n-2} + \ldots + \overline{r_n + L}) > 0,$$

et si l'on désigne par r le plus grand des coefficients, tous positifs, de la parenthèse, l'inégalité précédente sera vérifiée si l'on a

$$r_0\rho^n - r(\rho^{n-1} + \rho^{n-2} + \ldots + \rho + 1) > 0,$$

ou bien

$$r_0\rho^n - r\frac{\rho^n - 1}{\rho - 1} > 0,$$

et *a fortiori*, en supposant $\rho > 1$,

$$r_0\rho^n - \frac{r\rho^n}{\rho - 1} > 0;$$

il suffit donc de prendre

$$\mu = 1 + \frac{r}{r_0}.$$

En particulier, si l'on suppose $L = 0$, le nombre μ est tel que le polynôme ne peut s'annuler lorsque la valeur absolue de x surpasse μ, et l'on dit que μ est une limite supérieure des racines de l'équation $f(x) = 0$.

CHAPITRE X.

LE CALCUL DES PROBABILITÉS.

---

91. Probabilité et certitude. — La probabilité d'un événement est le rapport du nombre des *cas favorables* au nombre total des cas *possibles,* en supposant tous les cas également possibles et en nombre limité. Ainsi, la probabilité est un nombre fractionnaire compris entre les limites 0 et 1, qui sont respectivement les symboles de l'*impossibilité* et de la *certitude.* Le compte des cas favorables et des cas possibles appartient à l'analyse combinatoire qui suffit, en général, pour résoudre les premiers problèmes qui concernent les probabilités. Au moyen de quelques théorèmes fondamentaux, ce calcul n'est plus qu'un Chapitre particulier de l'Arithmétique, ou de la Doctrine des nombres entiers, comme celui de la Géométrie de situation.

Exemple I. — Un sac contient p boules blanches et q boules noires; quelle est la probabilité d'extraire, d'un seul coup, a boules blanches et b boules noires?

La probabilité cherchée est le rapport du produit $C_p^a C_q^b$ à C_{p+q}^{a+b}.

Exemple II. — *La loterie.* — Un sac contient p numéros et l'on en tire q; quelle est la probabilité d'obtenir r numéros désignés à l'avance?

La probabilité cherchée est le rapport de C_{p-r}^{q-r} à C_p^q. — Dans l'ancienne loterie, on avait $p = 90$ et $q = 5$; en faisant varier r de 1 à 5, la formule précédente donne la probabilité de l'*extrait*, de l'*ambe*, du *terne*, du *quaterne* et du *quine*.

Exemple III. — On tire trois boules d'un jeu de n lotos; quelle est la probabilité pour que l'un des nombres extraits soit égal à la somme ou à la demi-somme des deux autres?

Dans les deux cas, on trouve

Pour n pair........................ $\dfrac{3}{2n-1}$

Pour n impair..................... $\dfrac{3(n-1)}{2n(n-2)}$

Exemple IV. — Un sac renferme b boules blanches et n boules noires et l'on suppose $b > n$; on tire ces boules une à une et l'on demande la probabilité que, à aucun moment du tirage, le nombre des boules noires sorties n'aura dépassé celui des boules blanches.

Si l'on représente les boules blanches sorties par des pas verticaux $\downarrow$ sur un échiquier et celui des boules noires par des pas horizontaux $\rightarrow$, la probabilité cherchée sera, d'après la théorie de l'échiquier triangulaire de DELANNOY et du carré arithmétique de FERMAT (n[os] 53 et 54),

$$\frac{T_n^b}{F_n^b} = \frac{b-n-1}{b-1}.$$

Exemple V. — Un joueur a gagné n parties et en a perdu n: on demande la probabilité que ses pertes n'ont jamais dépassé ses gains.

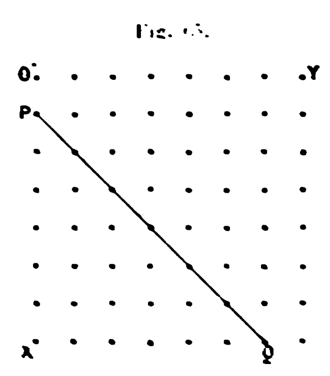
On a, comme ci-dessus, pour la probabilité cherchée, avec $b = n$,

$$\frac{T_n^n}{F_n^n} = \frac{1}{n-1}.$$

Exemple VI. — *Le scrutin de ballottage.* — Deux candidats sont soumis à un scrutin de ballottage: le premier, A, obtient a suffrages, est élu, et l'autre, B, n'obtient que b suffrages. On demande la probabilité pour que, pendant le dépouillement du scrutin, les voix de l'élu A ne cessent pas une seule fois de dépasser celles de son concurrent?

Représentons les voix de l'élu A par des pas verticaux $\downarrow$, et celles du candidat malheureux B par des pas horizontaux $\rightarrow$: le nombre total des manières dont peuvent se combiner les voix des deux candidats est égal

Fig. 65.



au nombre des marches de la tour pour se rendre sur la case de coordonnées (a, b) dans le carré arithmétique de FERMAT, c'est-à-dire à F_a^b. D'autre part, le nombre des dispositions du recensement des suffrages dans lesquelles les voix de A surpassent toujours celles de B est égal au nombre des manières dont la tour peut se rendre de l'origine O (*fig.* 65) à la case de

coordonnées (a, b), sans sortir de l'échiquier triangulaire PXQ de DELANNOY; la probabilité cherchée est donc

$$\frac{T_{a-1}^{b}}{F_{a}^{b}} = \frac{a-b}{a+b}.$$

Plus généralement, la probabilité pour que l'écart ne soit jamais inférieur à un nombre donné c est fournie par le rapport de T_{a-c}^{b} à F_{a}^{b}, ainsi qu'on le voit en baissant de $(c-1)$ rangs la ligne PQ.

D'autres solutions de ce problème ont été données par MM. J. BERTRAND et D. ANDRÉ, dans les *Comptes rendus de l'Académie des Sciences* (t. CV, p. 369 et 436; Paris, 1887).

92. Probabilité composée. — Lorsqu'un événement se compose du concours de deux ou de plusieurs événements simples, indépendants les uns des autres, la probabilité de l'événement composé est le produit des probabilités des événements simples.

Si un premier événement influe sur la probabilité d'un second, la probabilité de l'événement composé est le produit de la probabilité du premier par la probabilité *réduite* du second, c'est-à-dire celle qu'il acquiert quand le premier est arrivé.

93. Probabilité totale. — Lorsque les cas favorables à l'arrivée d'un événement peuvent se présenter de plusieurs manières qui s'excluent mutuellement, la probabilité de cet événement est égale à la somme des probabilités que l'événement se présentera de chacune de ces manières.

Ainsi, soit p_i la probabilité de l'événement lorsque la cause c_i agit certainement et exclusivement, et q_i la probabilité que cette cause est en jeu, la probabilité P de l'événement est

$$P = p_1 q_1 + p_2 q_2 + \ldots + p_i q_i + \ldots.$$

Exemple I. — Quelle est la probabilité d'amener un *as*, au moins une fois, en jetant deux dés?

Cette probabilité est

$$\frac{1}{6} \cdot \frac{5}{6} + \frac{1}{6} \cdot \frac{5}{6} + \frac{1}{6} \cdot \frac{1}{6} = \frac{11}{36}.$$

Exemple II. — Quelle est la probabilité qu'un joueur amène un *brelan* à la bouillotte?

On trouve

$$\frac{20}{20} \cdot \frac{3}{19} \cdot \frac{2}{18} \quad \text{ou} \quad \frac{1}{57}.$$

Exemple III. — Probabilité pour obtenir un as, une seule fois, en jetant quatre ou cinq dés.

On trouve

$$\frac{500}{1296} \quad \text{et} \quad \frac{3651}{7776}.$$

Exemple IV. — Quelle est la probabilité d'obtenir le point 7 avec deux dés, avant qu'aucun autre point se produise deux fois?

On trouve

$$\frac{7303}{13860}.$$

Exemple V. — On jette en l'air cinq pièces de monnaie; la probabilité pour qu'elles montrent trois piles et deux faces est égale à $\frac{5}{16}$.

Exemple VI. — Dans une loterie de 40000 billets, il y a trois lots; on prend 8000 billets. Quelles sont les probabilités d'obtenir un lot ou de les gagner tous les trois?

On trouve respectivement

$$\frac{61}{125} \quad \text{et} \quad \frac{1}{125}.$$

Exemple VII. — Une urne contient 10 boules blanches, 10 boules bleues et 10 boules rouges; on en prend trois au hasard. Quelle est la probabilité d'amener une boule de chaque couleur?

On trouve

$$\frac{100}{406}.$$

Exemple VIII. — En combien de coups peut-on parier, avec chance égale, que l'on amènera trois as deux fois, en jetant trois dés?

Il faut 361 coups.

Exemple IX. — En combien de coups, avec un seul dé, peut-on parier, avec chance égale, de voir les six faces?

En 13 coups.

Exemple X. — En combien de coups, avec deux dés, peut-on parier, avec chance égale, d'amener tous les doublets?

En 79 coups.

La plupart des exercices précédents sont empruntés à Moivre.

94. Théorème de Bayes. — Désignons par $p_1, p_2, p_3, \ldots$ les probabilités que des causes $c_1, c_2, c_3, \ldots$, qui s'excluent mutuellement, donnent respectivement à un événement, et par $q_1, q_2, q_3, \ldots$ les probabilités respectives de ces causes. Supposons que l'événement considéré ait été observé dans une épreuve, la proba-

bilité ϖ_i que l'arrivée de l'événement est due à la cause c_i est donnée par la formule

$$\varpi_i = \frac{p_i q_i}{p_1 q_1 + p_2 q_2 + \ldots}.$$

Exemple I. — Une urne contient b_1 boules blanches et n_1 boules noires; une deuxième urne contient b_2 boules blanches et n_2 boules noires, ...; une $r^{\text{ième}}$ urne contient b_r boules blanches et n_r boules noires. En tirant de ces r urnes une boule, celle-ci se trouve blanche. Quelle est la probabilité que cette boule est sortie de l'urne de rang i?

On trouve, par l'application du théorème de BAYES, pour numérateur et pour dénominateur de ϖ_i,

$$\frac{1}{r}\frac{b_i}{b_i + n_i}, \quad \text{et} \quad \sum \frac{1}{r}\frac{b_i}{b_i + n_i};$$

on a donc

$$\varpi_i = \frac{b_i}{b_i + n_i} : \sum \frac{b_i}{b_i + n_i}.$$

Exemple II. — Une urne contient cinq boules, les unes sont blanches, les autres sont noires, mais on ignore en quelle proportion. On tire six boules, en remettant après chaque tirage la boule sortie, et il ne sort que des boules blanches. Quelle est la probabilité pour que l'urne ne contienne que des boules blanches?

Supposons d'abord que toutes les combinaisons possibles des cinq boules, les unes blanches, les autres noires, aient été préparées dans des urnes d'apparence identique et que le hasard ait décidé le choix de l'une d'elles. Alors les probabilités $q_1, q_2, \ldots$ sont égales entre elles, et l'application du théorème de BAYES donne, pour la probabilité cherchée,

$$\frac{5^6}{1^6 + 2^6 + 3^6 + 4^6 + 5^6}.$$

Mais si l'on a composé l'urne, en tirant au sort, par le jeu de pile ou face, la couleur de chaque boule, les probabilités $q_1, q_2, \ldots,$ seront proportionnelles aux nombres 5, 10, 10, 5, 1, et la probabilité cherchée serait

$$\frac{5^6}{5.1^6 + 10.2^6 + 10.3^6 + 5.4^6 + 1.5^6}.$$

Exemple III. — Une urne contient a boules, noires ou blanches, dont on a tiré la couleur à pile ou face, avant de les introduire dans l'urne. En faisant μ tirages dans l'urne ainsi composée, on obtient b boules blanches et n boules noires. Quelle est la composition la plus probable de l'urne?

On trouve

$$\frac{a}{2}\frac{a + 2m}{a + \mu} \text{ blanches} \quad \text{et} \quad \frac{a}{2}\frac{a + 2n}{a + \mu} \text{ noires.}$$

95. Théorème de Jacques Bernoulli. — Soit p la probabilité d'un événement et a le nombre de fois qu'il se présente dans une suite de s épreuves; soit P la probabilité que la différence entre p et $(a : s)$ soit inférieure, en valeur absolue, à ε. On peut toujours prendre s assez grand pour que P diffère aussi peu qu'on voudra de l'unité.

Lorsque la probabilité d'un événement est variable d'une épreuve à l'autre, le théorème de BERNOULLI n'est plus applicable. La généralisation proposée par POISSON, sous le nom de *loi des grands nombres*, manque non seulement de rigueur, mais aussi de précision.

96. De l'espérance mathématique. — Lorsqu'un événement encore douteux doit amener un certain bénéfice, on appelle *espérance mathématique*, le produit de ce bénéfice par la probabilité de l'obtenir. Lorsque la somme espérée est connue, la recherche de la probabilité et celle de l'espérance mathématique forment un même problème. Mais, si des événements ayant pour probabilités respectives p_1, p_2, p_3, ... donnent droit aux sommes respectives s_1, s_2, s_3, ..., l'espérance mathématique est

$$p_1 s_1 + p_2 s_2 + p_3 s_3 + \dots.$$

Ainsi, l'espérance mathématique est connue lorsque l'on a calculé les probabilités respectives des divers cas possibles; mais, parfois, il est plus simple de calculer directement l'espérance.

Exemple I. — Pierre et Paul jouent au *jeu de rencontres*. Un sac contient μ boules numérotées de 1 à μ; Paul tire successivement les μ boules et s'engage à donner à Pierre 1fr chaque fois qu'un numéro sortira à son rang. Quelle est l'espérance mathématique de Pierre?

L'espérance est pour chaque tirage $\frac{1}{\mu}.1^{\text{fr}}$, et pour les μ tirages, elle est égale à 1fr. Nous calculerons plus loin, au Chapitre XIII, la probabilité du jeu des rencontres (n° 123).

Exemple II. — Pierre a trois pièces et Paul en a deux; ils conviennent que chacun jettera ses pièces en l'air et que celui qui obtiendra le plus grand nombre de faces prendra les cinq pièces. Le jeu est-il équitable?

Pierre a pour probabilité de *gagner*

$$\frac{1}{8}.0 + \frac{3}{8}.\frac{1}{4} + \frac{3}{8}.\frac{3}{4} + \frac{1}{8}.1 \quad \text{ou} \quad \frac{16}{32},$$

et pour probabilité de faire *partie nulle*,

$$\frac{1}{8}\cdot\frac{1}{4}+\frac{3}{8}\cdot\frac{2}{4}+\frac{3}{8}\cdot\frac{1}{4} \quad \text{ou} \quad \frac{10}{32};$$

son espérance mathématique est donc, en supposant les pièces de cinq francs,

$$25\cdot\frac{16}{32}+15\cdot\frac{10}{32}, \quad \text{ou} \quad \frac{5}{32}\cdot 110;$$

l'espérance mathématique de Paul est

$$25\cdot\frac{6}{32}+10\cdot\frac{10}{32}, \quad \text{ou} \quad \frac{5}{32}\cdot 50;$$

le jeu n'est pas équitable et favorise Pierre.

Exemple III. — Pierre et Paul jouent aux conditions suivantes. On jette deux dés sur le tapis; lorsqu'on amène un point au-dessous de 10, Paul donne à Pierre autant de francs que l'on a amené de points; dans le cas contraire, Pierre donne à Paul une somme fixe x qu'il s'agit de déterminer de telle sorte que le jeu soit équitable, c'est-à-dire que les espérances mathématiques des deux joueurs soient égales?

L'espérance mathématique de Pierre est

$$2\cdot\frac{1}{36}+3\cdot\frac{2}{36}+4\cdot\frac{3}{36}+5\cdot\frac{4}{36}+6\cdot\frac{5}{36}+7\cdot\frac{6}{36}+8\cdot\frac{5}{36}+9\cdot\frac{4}{36}, \quad \text{ou} \quad \frac{188}{36};$$

celle de Paul est

$$x\left(\frac{3}{36}+\frac{2}{36}+\frac{1}{36}\right) \quad \text{ou} \quad \frac{6}{36}x.$$

Par conséquent

$$x=\frac{188}{6}.$$

Exemple IV. — Un sac contient a boules blanches et $(n-a)$ boules noires. Un joueur tire les boules, une à une, jusqu'à ce qu'il amène p boules blanches, et reçoit 1[fr] par boule blanche tirée. Quelle est son espérance mathématique?

Si l'on remet la boule dans le sac, après chaque tirage, l'espérance mathématique du joueur est égale à

$$p\frac{n}{a};$$

mais, lorsqu'on ne remet pas dans le sac les boules tirées, l'espérance mathématique a pour expression

$$p\frac{n+1}{a+1}.$$

97. Des jeux de hasard. — On appelle ainsi les jeux, tels que le jeu de dés, [illegible], dans lesquels la perte ou le gain ne dépendent ni de l'adresse, ni du talent, ni d'aucune qualité inhérente aux joueurs, ni même de circonstances connues d'eux, mais seulement du hasard, dont ils ne peuvent nullement calculer les effets.

Pour qu'un jeu soit équitable, il faut que l'espérance mathématique de chaque joueur soit égale à sa mise qu'il livre au jeu, ne lui appartient plus.

Ordinairement la somme éventuelle attendue par chaque joueur est la mise totale des joueurs; dans ce cas, la mise de chaque joueur doit être proportionnelle à la chance qu'il a de gagner.

98. Sur l'effet des jeux de hasard. — Ruine des joueurs. — Si deux joueurs A et B possèdent respectivement a et b francs et jouent ensemble à un jeu équitable, le plus riche des deux joueurs ruinera probablement l'autre, car leurs probabilités de se ruiner l'un l'autre sont respectivement

$$\frac{a}{a-b} \quad \text{et} \quad \frac{b}{a-b}.$$

Si le joueur B représente le public, b est plus grand que tout nombre donné, a, si grand qu'il soit; alors *la ruine d'un joueur quelconque* A *est certaine.*

Le seul cas dans lequel la ruine ne soit pas certaine est celui où le jeu n'est pas équitable. L'avantage, quelque petit qu'il soit, fait disparaître la certitude de ruine : c'est le cas du banquier dans les jeux publics. Un avantage est, pour lui, juste et nécessaire : mais il importe de ne pas l'exagérer.

Exemple I. — Un joueur expose à un jeu de hasard la $n^{\text{ième}}$ partie de sa fortune et renouvelle l'épreuve indéfiniment. Quelle est la probabilité pour qu'il se ruine et que la $2\mu - n^{\text{ième}}$ partie jouée lui enlève son dernier écu?

Désignons par x le nombre des parties perdues par le joueur et par y celui des parties gagnées; d'après les données du problème, x et y doivent vérifier les conditions

$$x - y = \lambda - \mu,$$

en posant

$$x - y = n,$$

et, pour abréger,

$$\mu - n = \lambda.$$

Pour que le joueur soit ruiné après la $(\lambda+\mu)^{\text{ième}}$ partie, et pas avant, il faut et il suffit :

1° Que, pendant le cours des $(\lambda+\mu-1)$ premières parties, ses pertes n'aient jamais dépassé ses gains de plus de $(n-1)$;

2° Qu'après les $(\lambda+\mu-1)$ premières parties, l'excès de ses pertes sur ses gains soit égal à $(n-1)$;

3° Qu'il perde la $(\lambda+\mu)^{\text{ième}}$ partie.

Soient ϖ_1, ϖ_2, ϖ_3 les probabilités correspondantes, et Π la probabilité composée ; on a

$$\Pi = \varpi_1 \varpi_2 \varpi_3.$$

En se reportant aux notations des échiquiers arithmétiques (n°s 53 et 55), et en représentant par $\downarrow$ et $\rightarrow$ les gains et les pertes, on a

$$\varpi_1 = \frac{P^y_{x-1}}{F^y_{x-1}}, \qquad \varpi_2 = \frac{F^y_{x-1}}{2^{\lambda+\mu-1}}, \qquad \varpi_3 = \frac{1}{2};$$

par suite,

$$\Pi = \frac{P^y_{x-1}}{2^{\lambda+\mu}} = \frac{n}{2^{\lambda+\mu}} \frac{(\lambda+\mu-1)!}{\lambda!\mu!}.$$

Cette question de la *durée du jeu* a été traitée autrement par HUYGENS, MOIVRE, LAPLACE, LAGRANGE, AMPÈRE et, tout récemment, par M. J. BERTRAND (*Comptes rendus de l'Académie des Sciences*, t. CV, p. 437; 1887).

Exemple II. — Pierre et Paul jouent à un jeu de hasard, la probabilité de gagner chaque partie étant p pour Pierre et q pour Paul. Les enjeux de Pierre et de Paul sont respectivement a et b francs, et leurs fortunes sont m et n. Quel est le nombre probable des parties qui seront jouées avant la ruine de l'un des joueurs, en supposant le jeu équitable?

C'est l'entier du quotient de mn par ab. — Si le jeu n'est pas équitable, et si l'on désigne par ϖ la probabilité calculée pour que Pierre finisse par ruiner Paul, le nombre des parties est l'entier de

$$\frac{(m+n)\varpi - n}{pb - qa}.$$

Exemple III. — Pierre et Paul jouent l'un contre l'autre avec des probabilités égales. Ils possèdent chacun n francs avant d'entrer au jeu; à chaque partie, le perdant donne 1 franc au gagnant, et le jeu ne cesse que lorsqu'un des joueurs est ruiné. Quelle est la probabilité Π pour que le jeu se termine à la fin de la $\mu^{\text{ième}}$ partie?

Pour que l'un des joueurs soit ruiné après cette $\mu^{\text{ième}}$ partie, et pas avant, il faut et il suffit :

1° Que, pendant le cours des $(\mu-1)$ premières parties, l'écart entre les pertes et les gains de chaque joueur n'ait jamais dépassé $(n-1)$;

2° Qu'après les $(\mu-1)$ premières parties, l'excès des pertes sur les gains de l'un des joueurs soit égal à $(n-1)$;

3° Que la dernière partie soit perdue par le joueur qui ne possède plus que 1^fr.

Soient $\varpi_1, \varpi_2, \varpi_3$ les probabilités correspondantes, et Π la probabilité cherchée. Nous remarquerons d'abord que, pour la possibilité du problème, il faut supposer μ et n de même parité. Soit donc

$$(1) \qquad \mu + n = 2\kappa, \qquad \mu - n = 2\lambda;$$

on a

$$\varpi_2 = 2\frac{C_{\mu-1}^{\lambda}}{2^{\mu-1}} \qquad \text{et} \qquad \varpi_3 = \frac{1}{2},$$

Il nous reste à déterminer la valeur de ϖ_1. Désignons par x et y les nombres des parties perdues et gagnées par l'un des joueurs; représentons les pertes par des pas verticaux $\downarrow$ sur un échiquier et les gains par des pas horizontaux $\rightarrow$. Le nombre des dispositions des x et des y, telles que l'écart entre les gains et les pertes, ne dépasse pas $(n-1)$, est égal au nombre des marches d'une tour, par pas successifs, de l'origine à la case (x, y), sur l'échiquier hexagonal (n° 56), dans lequel on suppose

$$a = b = (n-1).$$

Ainsi ϖ_1 est le rapport de H_x^{λ} à F_x^{y}; mais, pour la case (x, y) dont les coordonnées vérifient les relations

$$x + y = \mu - 1, \qquad x - y = n - 1,$$

d'où $x = \kappa - 1$ et $y = \lambda$, on a

$$H_x^{\lambda} = \frac{n}{\kappa}\left[C_{\mu-1}^{\lambda} - \frac{3n}{\kappa+n} C_{\mu-1}^{\lambda-n} + \ldots + (-1)^h \frac{(2h+1)n}{\kappa+hn} C_{\mu-1}^{\lambda-hn}\right],$$

ou encore

$$H_x^{y} = \frac{n}{\mu}\left[C_{\mu}^{\lambda} - 3C_{\mu}^{\lambda-n} + \ldots + (-1)^h (2h+1) C_{\mu}^{\lambda-hn}\right],$$

en désignant par hn le plus grand multiple de n contenu dans λ. Par suite, on a

$$\Pi = \frac{n}{\mu . 2^{\mu-1}}\left[C_{\mu}^{\lambda} - 3C_{\mu}^{\lambda-n} + \ldots + (-1)^h (2h+1) C_{\mu}^{\lambda-hn}\right].$$

Exemple IV. — A et B jouent l'un contre l'autre avec des probabilités p et q; ils possèdent respectivement a et b francs avant d'entrer au jeu. A chaque partie, le perdant donne un franc au gagnant et le jeu ne cesse que lorsque l'un des deux joueurs est ruiné. On demande la probabilité Π pour que le jeu se termine juste à la fin d'une partie de rang assigné.

Soit μ le rang assigné à la partie finale. En désignant par Π_A et Π_B les probabilités respectives que A ou B seront ruinés après la $\mu^{\text{ième}}$ partie, et pas avant, on aura

$$\Pi = \Pi_A + \Pi_B.$$

En raisonnant comme à l'exemple précédent, on a

$$\Pi_A = \frac{H^y_{x-1}}{F^y_{x-1}} \times p^{x-1} q^y F^y_{x-1} \times p = p^x q^y H^y_{x-1}.$$

Si l'on pose

$$\mu - a = 2r, \qquad \mu + a = 2s, \qquad a + b = d,$$

on a

$$\Pi_A = p^s q^r \sum \left[\frac{2hd + a}{s + hd} C^{r-hd}_{\mu-1} - \frac{(2h+1)d + b}{s + hd + b} C^{r-hd-b}_{\mu-1} \right],$$

ou bien

$$\Pi_A = p^s q^r \sum \left[\frac{2hd - a}{r - hd} C^{r-hd-1}_{\mu-1} - \frac{(2h+1)d + b}{r - hd - b} C^{r-hd-b-1}_{\mu-1} \right];$$

pour toutes les valeurs de h,

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad E\frac{r}{d}.$$

Exemple V. — A joue contre B; à chaque partie, les probabilités qu'ils ont respectivement de gagner sont p et q, en sorte que $p + q = 1$, et le perdant donne un franc au gagnant. En entrant au jeu, les joueurs possèdent respectivement a et b francs. On demande la probabilité que A ruinera B avant le coup de rang μ.

On trouve, par l'échiquier hexagonal (n° 36),

$$\Pi = p^b \Sigma (pq)^\lambda H^{b+\lambda-1}_\lambda,$$

en faisant varier λ de 0 à $\frac{1}{2}(\mu - b) - 1$. On voit facilement que si

λ varie de	0	à	$a - 1$,	Π possède	1	terme;
»	a	à	$a - 1 + b$,	»	2	termes;
»	$a + b$	à	$2a - 1 + b$,	»	3	»
»	$2a + b$	à	$2a - 1 + 2b$,	»	4	»
.....	.....	.....	.....	.....	.....	.....

Dans son *Traité du Calcul des Probabilités* (p. 81), M. LAURENT donne une solution pour le cas où a et b vérifient la relation

$$b = qa + pa^{-1}.$$

Exemple VI. — *Carré arithmétique de* DELANNOY. — De combien de

En particulier, dans l'échiquier pentagonal, pour les termes de la transversale située au-dessous des zéros, on a

$$y = x + b + 1$$

et, par suite,

$$H_x^y = \frac{b}{y + 1 - x} \Phi_x^y.$$

Exemple VII. — Deux joueurs d'échecs marquent, au fur et à mesure, les parties qu'ils gagnent et celles qu'ils perdent; de plus, à chaque partie nulle, chacun des joueurs marque une partie gagnée et une partie perdue. Après avoir marqué ainsi chacun $2n$ parties, ils n'ont ni gain ni perte. On demande la probabilité qu'ils auront joué $2n$ parties effectives, c'est-à-dire qu'il n'y aura pas eu de partie nulle.

Si l'on désigne les parties de l'un des joueurs par des pas horizontaux, diagonaux, verticaux, suivant que la partie a été gagnée, nulle ou perdue, la considération de l'échiquier Φ montre que la probabilité cherchée est le quotient de F_n^n par Φ_n^n.

CHAPITRE XI.

LA DIVISION ALGÉBRIQUE.

99. Division des polynômes ordonnés suivant les exposants décroissants. — Diviser un polynôme $f(x)$ par un polynôme $g(x)$ revient à trouver deux autres polynômes Q et R, de telle sorte que l'on ait l'identité

$$f(x) = Qg(x) + R,$$

le degré de $g(x)$ étant au plus égal à celui de $f(x)$, et le degré de R étant plus petit que celui de $g(x)$.

Cette transformation n'est possible que d'une seule manière, en supposant les deux polynômes ordonnés suivant les exposants décroissants de x.

Opération de la division algébrique.

100. Division d'un polynôme par $(x - a)$. — Nous avons appris à calculer le quotient aux n°s 71 et 72,

$$f_0 x^{n-1} + f_1 x^{n-2} + f_2 x^{n-3} + \ldots + f_{n-1};$$

les coefficients $f_0, f_1, f_2, \ldots, f_{n-1}$ se calculent successivement au moyen du précédent, et le reste de la division de $f(x)$ par $(x - a)$ est $f(a)$.

Exemple I. — Division de $f(x)$ par $(x \mp 1)$. — Reste de la division d'un nombre entier par 9 et par 11 dans le système décimal, et plus généralement par $(b \mp 1)$ dans le système de numération de base b.

Exemple II. — Division de $(x^m \mp a^m)$ par $(x \mp a)$. — Quatre cas.

Exemple III. — Division de $f(x)$ par $(bx - a)$. — Calculs du reste et du quotient.

Exemple IV. — Reste de la division de $f(x)$ par $(x^p \mp a)$. — Reste de la division d'un nombre entier par 99, par 999, ... et par 101, par 1001, ... dans le système décimal, et plus généralement par $(b^p \mp 1)$ d'un nombre écrit dans le système de numération de base b.

Exemple V. — Division de $(x^n - a^n)$ par $(x^p - a^p)$. — Le reste est

$$a^{pq}(x^r - a^r),$$

en désignant par q et par r le quotient et le reste de la division de n par p.

Exemple VI. — Division d'un nombre entier par 19. — On applique la règle de la division de $f(x)$ par $(x - \frac{1}{2})$, pour $x = 10$. Ainsi, on a tout de suite

$$\frac{10^{18}-1}{19} = 5.{}^{1}2.6.3.{}^{1}1.{}^{1}5.{}^{1}7.{}^{1}8.9.{}^{1}4.7.{}^{1}3.{}^{1}6.8.4.2.1;$$

chaque chiffre est la moitié du précédent, ou la moitié du précédent augmenté de 10, si la division antérieure donne pour reste 1; c'est ce dernier cas que nous avons indiqué par un petit chiffre 1 placé au-dessus et à gauche. On opère de même pour $x = 100$, $x = 1000$, ..., en calculant par groupes de deux, trois, ... chiffres; ainsi

$$\frac{10^{198}-1}{199} = 50.25.{}^{1}12.56.28.14.07.03.{}^{1}51.{}^{1}75.{}^{1}87.{}^{1}93.{}^{1}96.98\ldots,$$

$$\frac{10^{1998}-1}{1999} = 500.250.125.{}^{1}062.531.{}^{1}265.{}^{1}632.816.408.204.102\ldots;$$

on connaît de même des procédés rapides pour la division par 29, 39, 49, ...; par 299, 399, 499, ...; etc.

Exemple VII. — L'expression

$$k = 2^{[illegible]} - 2^{[illegible]} - 1$$

est toujours divisible par 9 et le quotient est un nombre triangulaire. En effet, on a

$$\frac{k}{9} = \frac{\alpha(\alpha-1)}{2} \qquad \text{et} \qquad \alpha = 2\,\frac{4^{n}-1}{4-1}.$$

101. Division d'un polynôme par un produit de binômes. — Si l'on désigne par $A(x)$ et $B(x)$ les quotients, que l'on sait former, dans la division de $f(x)$ par $(x-a)$ et par $(x-b)$, et si l'on désigne par $\alpha = f(a)$ et $\beta = f(b)$ les restes des deux divisions, on a

$$\frac{f(x)}{x-a} = A(x) + \frac{\alpha}{x-a},$$

$$\frac{f(x)}{x-b} = B(x) + \frac{\beta}{x-b};$$

donc, par soustraction, en supposant $a \gtrless b$,

$$\frac{f(x)}{(x-a)(x-b)} = \frac{A(x)-B(x)}{a-b} + \frac{1}{a-b}\,\frac{x(\alpha-\beta)+a\beta-b\alpha}{(x-a)(x-b)}.$$

De même, connaissant les quotients et les restes des divisions de $f(x)$ par $(x-a)(x-b)$, et par $(x-a)(x-c)$, en supposant a, b, c inégaux deux à deux, on calculera le quotient et le reste de la division de $f(x)$ par le produit $(x-a)(x-b)(x-c)$, en faisant la différence

$$\frac{f(x)}{(x-a)(x-b)} - \frac{f(x)}{(x-a)(x-c)},$$

et en divisant par $(b-c)$. Ces calculs seront généralisés dans la théorie de l'interpolation et dans celle de la décomposition des fractions rationnelles.

Exemple I. — Lorsqu'un polynôme entier est divisible par $(x-a)^\alpha$, par $(x-b)^\beta$, par $(x-c)^\gamma$, ..., en désignant par $a, b, c, \ldots$ des nombres inégaux deux à deux, il est divisible par le produit

$$(x-a)^\alpha (x-b)^\beta (x-c)^\gamma \ldots.$$

Exemple II. — Si un polynôme entier en x, y, z est séparément divisible par les binômes $(x-y)$, $(y-z)$, $(z-x)$, il est divisible par leur produit.

Exemple III. — Démontrer qu'un polynôme entier et symétrique en x et y, divisible par $(x-y)$, est divisible par $(x-y)^2$. Généraliser pour un polynôme à trois variables.

Exemple IV. — Pour que

$$x^m + y^m + z^m - (x+y+z)^m$$

soit divisible par le produit

$$(y+z)(z+x)(x+y),$$

il faut et il suffit que m soit impair. — Former le quotient.

Exemple V. — Démontrer que

$$y^p z^q + z^p x^q + x^p y^q - y^q z^p - z^q x^p - x^q y^p$$

et que

$$x^p y^q z^r + y^p z^q x^r + z^p x^q y^r - x^p y^r z^q - y^p z^r x^q - z^p x^r y^q$$

sont divisibles par le produit

$$(y-z)(z-x)(x-y).$$

Exemple VI. — Décomposer en facteurs les expressions

$$(y-z)^3+(z-x)^3+(x-y)^3,$$
$$x^3(y-z)+y^3(z-x)+z^3(x-y),$$
$$x^3(z-y^2)+y^3(x-z^2)+z^3(y-x^2)+xyz(xyz-1).$$

Exemple VII. — Démontrer que

$$(x+y+z)^{2n+1}-x^{2n+1}-y^{2n+1}-z^{2n+1}$$

est divisible par

$$(x+y+z)^3-x^3-y^3-z^3.$$

102. Expression d'un polynôme de degré n comme somme algébrique de polynômes. — Si l'on désigne par $f(x)$ un polynôme de degré n, et par

$$\varphi_n(x),\quad \varphi_{n-1}(x),\quad \ldots,\quad \varphi_1(x),\quad \varphi_0$$

une suite de polynômes donnés dont les degrés reproduisent la série complète des n premiers nombres entiers, le polynôme $f(x)$ peut être transformé en une somme de ces polynômes multipliés respectivement par des coefficients indépendants de x. En d'autres termes, on a l'identité

$$f(x)=\lambda_0\varphi_n+\lambda_1\varphi_{n-1}+\lambda_2\varphi_{n-2}+\ldots+\lambda_n\varphi_0,$$

dans laquelle les quantités $\lambda_0, \lambda_1, \lambda_2, \ldots, \lambda_n$ sont des constantes, dont la première n'est jamais nulle.

Pour effectuer cette transformation, on divise $f(x)$ par $\varphi_n(x)$; on obtient pour quotient λ_0 et l'on divise le reste par $\varphi_{n-1}(x)$, ce qui donne λ_1, et ainsi de suite. D'ailleurs, cette transformation, toujours possible, n'est possible que d'une seule manière pour une suite complète donnée des polynômes $\varphi(x)$. Lorsque ces polynômes représentent les puissances de x,

$$x^n,\quad x^{n-1},\quad x^{n-2},\quad \ldots,\quad x^2,\quad x,\quad 1,$$

les constantes λ sont précisément égales aux coefficients de $f(x)$.

Exemple I. — Convertir, dans un système de base donnée, un nombre écrit dans le système décimal.

Voici un moyen assez rapide indiqué par Legendre dans la *Théorie des nombres,* pour exprimer un nombre du système décimal en caractères bi-

naires. Soit, par exemple, le nombre 11 183 445; en le divisant par 64, on trouve le reste 21 et le quotient 174741. Ce dernier nombre divisé par 64 donne le reste 21 et le quotient 2730. Enfin 2730 divisé par 64 donne le reste 42 et le quotient 42. Mais 21 et 42 s'expriment dans le système binaire par

$$010101 \quad \text{et} \quad 101010;$$

donc le nombre proposé s'écrit dans la numération binaire

$$101010\ 101010\ 010101\ 010101.$$

Exemple II. — Quels que soient les n nombres $a, b, c, \ldots, l$, on a l'identité

$$(-1)^n \frac{(x-a)(x-b)\ldots(x-l)}{ab\ldots l}$$
$$= 1 - \frac{x}{a} + \frac{x(x-a)}{ab} - \ldots + (-1)^n \frac{x(x-a)\ldots(x-k)}{ab\ldots kl}.$$

103. Division des polynômes ordonnés suivant les exposants croissants. — Diviser un polynôme

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$

par un polynôme

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots$$

revient à trouver, pour les valeurs successives, entières et positives de p, des polynômes $Q_p(x)$ de degré p, de telle sorte que

$$(1) \qquad f(x) = Q_p(x)\, g(x) + x^{p+1} R_p(x),$$

$R_p(x)$ désignant un polynôme ordonné suivant les exposants positifs et croissants.

L'identité n'est possible que d'une seule manière, pour une valeur déterminée de p; en d'autres termes, si Q et Q' désignent des polynômes de degrés p, R et R' des polynômes entiers, les égalités

$$f(x) = Q g(x) + x^{p+1} R,$$
$$f(x) = Q' g(x) + x^{p+1} R'$$

entraînent l'identité de Q et de Q', et celle de R et de R'.

De l'identité (1), on déduit

$$\frac{f(x)}{g(x)} = Q(x) + x^{p+1} \frac{R(x)}{g(x)},$$

qui conduit au développement d'une fraction rationnelle suivant les exposants croissants de la variable x.

On peut donc *développer une fraction rationnelle sous la forme d'un polynôme entier de degré p augmenté d'un terme complémentaire,* égal au produit de x^{p+1} par une fraction rationnelle qui reste finie pour $x = 0$; le développement n'est possible que d'une seule manière. Lorsque $g(x)$ est divisible par x^α, on met $x^{-\alpha}$ en facteur.

On peut aussi développer une fraction rationnelle suivant les exposants décroissants. Soient

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$
$$g(x) = b_0 x^n + b_1 x^{n-1} + \ldots + a_n;$$

si l'on pose $x = y^{-1}$, on a

$$\frac{f(x)}{g(x)} = x^{m-n} \frac{a_0 + a_1 y + \ldots + a_m y^m}{b_0 + b_1 y + \ldots + b_n y^n}.$$

On développe la fraction rationnelle en y suivant les exposants croissants, et l'on remplace ensuite y par x^{-1}. La décomposition n'est possible que d'une seule manière.

Exemple I. — Si $f(x)$ est un polynôme ordonné suivant les exposants croissants de x

$$f(x) = 1 + ax + bx^2 + cx^3 + \ldots,$$

les coefficients du quotient de $f(x)$ par $(1 - x)$ sont successivement

$$1, \quad 1 + a, \quad 1 + a + b, \quad 1 + a + b + c, \quad \ldots.$$

La méthode de division par $9 = (10 - 1)$ dans le système décimal, que nous avons indiquée au n° 27 (*Ex. V*), est un cas particulier de ce résultat.

On déduit les développements

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \ldots + R,$$
$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + 4x^3 + \ldots + R',$$
$$\frac{1}{(1-x)^3} = 1 + 3x + 6x^2 + 10x^3 + \ldots + R'',$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

Le Tableau des coefficients reproduit, au signe près, le triangle de PAS-

CAL, pour les indices négatifs; on en déduit que *la formule du binôme de* NEWTON *s'applique aux exposants entiers et négatifs, en tenant compte d'un terme complémentaire,* et l'on a

$$\frac{1}{(1-x)^p} = 1 + \frac{p}{1}x + \frac{p(p+1)}{2}x^2 + \frac{p(p+1)(p+2)}{1.2.3}x^3 + \ldots + R.$$

Pour $-1 < x < 1$, le développement est convergent.

Exemple II. — Démontrer, pour n entier positif, la formule due à EULER,

$$(1+x)^n = 1 + \frac{n}{1}x + \frac{n(n-1)}{1.2}\frac{x^2}{1+x} + \frac{(n+1)n(n-1)}{1.2.3}\frac{x^3}{1+x} + \frac{(n+1)n(n-1)(n-2)}{1.2.3.4}\frac{x^4}{1+x} + \ldots$$

104. Méthode des coefficients indéterminés. — Si l'on veut développer la fonction

$$f(x) = (1+ax)(1+a^2x)\ldots(1+a^nx),$$

suivant les puissances de x, on pose

$$f(x) = 1 + A_1x + A_2x^2 + \ldots + A_nx^n,$$

et il s'agit de déterminer les coefficients $A_1, A_2, \ldots, A_n$, en observant que le développement est unique. On a l'identité

$$(1+ax)f(ax) = (1+a^{n+1}x)f(x);$$

remplaçons $f(ax)$ et $f(x)$ par leurs développements; égalons successivement les coefficients de $x, x^2, x^3, \ldots, x^n$, il vient, pour les coefficients de x^p,

$$a^pA_{p-1} + a^pA_p = a^{n+1}A_{p-1} + A_p;$$

d'où l'on tire

$$(1) \qquad A_p = A_{p-1}\frac{a^{n+1}-a^p}{a^p-1}$$

et, par suite,

$$(2) \qquad A_p = \frac{(a^n-1)(a^{n-1}-1)\ldots(a^{n-p+1}-1)}{(a-1)(a^2-1)\ldots(a^p-1)}a^{p(p+1)}.$$

Pour $a=1$, on retrouve la formule du développement de la puissance $(1+x)^p$ du binôme. Ce calcul est d'EULER.

On peut développer de même le produit

$$\varphi(x) = (1+ax)(1+a^3x)\dots(1+a^{2n-1}x),$$

en partant de l'identité

$$(1+a^2x)\varphi(ax) = (1+a^{2n+1}x)\varphi(x).$$

Exemple I. — Si l'on pose

$$\Gamma_n^p = \frac{(1-x^n)(1-x^{n-1})\dots(1-x^{n-p+1})}{(1-x)(1-x^2)\dots(1-x^p)},$$

l'expression Γ_n^p est un polynôme entier en x, ainsi que cela résulte de la formule (2), et l'on a l'identité

$$\Gamma_n^p = \Gamma_{n-1}^p + x^{n-p}\Gamma_{n-1}^{p-1},$$

analogue à la loi de formation du triangle arithmétique (n° 4).

Exemple II. — Si l'on pose, avec les notations précédentes,

$$f(x, n) = 1 - \Gamma_n^1 + \Gamma_n^2 - \dots + (-1)^n\Gamma_n^n,$$

on a la relation

$$f(x, n+2) = (1-x^{n+1})f(x, n);$$

par suite,

$$f(x, 2p+1) = 0,$$
$$f(x, 2p) = (1-x)(1-x^3)\dots(1-x^{2p-1}),$$
$$f(x, -2p)f\left(\frac{1}{x}, 2p\right) = 1.$$

Les exercices précédents sont dus à Gauss.

Exemple III. — On a l'identité

$$\frac{x}{1-x^2} + \frac{x^2}{1-x^4} + \dots + \frac{x^{2^{n-1}}}{1-x^{2^n}} = \frac{1}{1-x}\,\frac{x-x^{2^n}}{1-x^{2^n}}.$$

Exemple IV. — On a l'identité

$$\frac{x-x^q}{(1-x)(1-x^q)} + \frac{x^q-x^{pq}}{(1-x^q)(1-x^{pq})} = \frac{x-x^{pq}}{(1-x)(1-x^{pq})};$$

si l'on remplace q par p^n, et si l'on fait successivement n égal à 1, 2, 3, ..., n, la somme des égalités ainsi obtenues donne l'identité

$$\frac{x-x^p}{(1-x)(1-x^p)} + \frac{x^p-x^{p^2}}{(1-x^p)(1-x^{p^2})} + \dots + \frac{x^{p^n}-x^{p^{n+1}}}{(1-x^{p^n})(1-x^{p^{n+1}})}$$
$$= \frac{x-x^{p^{n+1}}}{(1-x)(1-x^{p^{n+1}})}.$$

Exemple V. — Si l'on pose

$$f_p = (1-x)(1-x^2)\ldots(1-x^p),$$

on a l'identité suivante, due à M. CESARO :

$$\frac{1}{f_p} - \frac{x}{f_1 f_{p-1}} + \frac{x^2}{f_2 f_{p-2}} + \ldots + \frac{(-1)^p x^{\frac{p(p+1)}{2}}}{f_p} = 1.$$

L'INTERPOLATION.

105. Formule d'interpolation de Lagrange. — Cette formule sert à résoudre le problème de trouver tous les polynômes $F(x)$ qui prennent des valeurs données

$$y_0,\quad y_1,\quad y_2,\quad \ldots,\quad y_n$$

pour $(n+1)$ valeurs inégales deux à deux de la variable x,

$$x_0,\quad x_1,\quad x_2,\quad \ldots,\quad x_n.$$

Considérons d'abord le polynôme $\varphi(x)$, de degré $(n+1)$,

$$\varphi(x) = (x-x_0)(x-x_1)\ldots(x-x_n):$$

il s'annule pour toutes les valeurs données de x. Désignons par x_k l'une d'elles; le polynôme X_k, de degré n,

$$X_k = \frac{\varphi(x)}{x-x_k}$$

s'annule pour toutes les valeurs données de x, à l'exception de $x = x_k$, pour laquelle il devient

$$A_k = (x_k - x_0)\ldots(x_k - x_{k-1})(x_k - x_{k+1})\ldots(x_k - x_n),$$

et A_k n'est pas nul. Par suite, pour $x = x_k$, le polynôme

$$y_k \frac{X_k}{A_k}$$

prend la valeur convenue et s'annule pour toutes les autres valeurs de x. Cela posé, le polynôme

$$f(x) = y_0 \frac{X_0}{A_0} + y_1 \frac{X_1}{A_1} + \ldots + y_n \frac{X_n}{A_n}$$

remplit les conditions demandées. Il est au plus de degré n, et se réduirait à une constante si toutes les quantités y étaient égales, puisque $f(x) - y_1$ s'annulerait pour $n+1$ valeurs de x.

Tous les autres polynômes $F(x)$ qui vérifient les conditions imposées sont d'ailleurs donnés par l'expression générale

$$F(x) = f(x) + \varphi(x)\,Q(x),$$

dans laquelle $Q(x)$ désigne un polynôme quelconque, puisque la différence

$$F(x) - f(x)$$

s'annule pour toutes les valeurs données de x : elle est donc divisible par $\varphi(x)$.

Inversement, si $f(x)$ est un polynôme quelconque, on a l'identité

$$(1)\qquad f(x) = \frac{f(x_0)}{X'_0}X_0 + \frac{f(x_1)}{X'_1}X_1 + \ldots + \frac{f(x_n)}{X'_n}X_n + \varphi(x)\,Q(x),$$

et aussi

$$\frac{f(x)}{\varphi(x)} = \frac{f(x_0)}{X'_0}\,\frac{1}{x - x_0} + \frac{f(x_1)}{X'_1}\,\frac{1}{x - x_1} + \ldots + Q(x).$$

La démonstration précédente est due à CAUCHY (*Cours d'Analyse algébrique*).

Exemple I. — Équation de la droite qui joint deux points donnés par leurs coordonnées.

On a

$$y = y_0\,\frac{x - x_1}{x_0 - x_1} + y_1\,\frac{x - x_0}{x_1 - x_0},$$

ou bien

$$y = x\,\frac{y_0 - y_1}{x_0 - x_1} + \frac{x_0 y_1 - x_1 y_0}{x_0 - x_1}.$$

L'intersection avec l'axe des x donne

$$x' = \frac{x_1 y_0 - y_1 x_0}{y_0 - y_1};$$

ce qui conduit à la formule d'interpolation par les parties proportionnelles. — *Règle de fausse position.* — Méthode d'HIPPARQUE.

Exemple II. — Trouver le reste de la division d'un polynôme $F(x)$ par le produit

$$(x - x_0)(x - x_1)\ldots(x - x_n).$$

C'est le polynôme $f(x)$ de degré n, au plus, qui prend pour $x = x_0$, $x_1, \ldots, x_n$, les valeurs $F(x_0)$, $F(x_1)$, $\ldots$, $F(x_n)$.

Exemple III. — Les trois fractions

$$(A) \qquad 2^n \frac{(2x+1)(2x+3)\ldots(2x+2n-1)}{x(x+1)\ldots(x+n)},$$

$$(B) \qquad \frac{1}{x(1^2-x^2)(2^2-x^2)\ldots(n^2-x^2)},$$

$$(C) \qquad 2^{2n} \frac{(1^2-2^2x^2)(3^2-2^2x^2)\ldots(\overline{2n-1}^2-2^2x^2)}{x(1^2-x^2)(2^2-x^2)\ldots(n^2-x^2)}$$

sont respectivement égales aux trois expressions

$$(A) \qquad \frac{(2n)!}{(n!)^2}\frac{1}{x} + \sum_{p=1}^{p=n} \frac{(2p)!(2n-2p)!}{[p!(n-p)!]^2}\frac{1}{x+p},$$

$$(B) \quad \frac{1}{(n!)^2}\frac{1}{x} + \sum_{p=1}^{p=n}(-1)^p \frac{1}{(n-p)!(n+p)!}\left[\frac{1}{x-p} + \frac{1}{x+p}\right],$$

$$(C) \quad \frac{(2n)!(2n)!}{(n!)^4}\frac{1}{x} + \sum_{p=1}^{p=n}\frac{(2n-2p)!(2n+2p)!}{[(n-p)!(n+p)!]^2}\left[\frac{1}{x-p} + \frac{1}{x+p}\right].$$

Exemple IV. — Si l'on pose

$$G_n = \frac{n^{n-1}}{n!},$$

on a les identités

$$G_1 G_{2n} + G_2 G_{2n-1} + \ldots + G_n G_{n+1} = \frac{2n}{2n+1} G_{2n+1},$$

$$G_1 G_{2n+1} + G_2 G_{2n} + \ldots + \frac{1}{2}(G_{n+1})^2 = \frac{2n+1}{2n+2} G_{2n+2}.$$

Exemple V. — Si l'on pose

$$(2n)!\, A_n = x^2(x^2+2^2)(x^2+4^2)\ldots(x^2+\overline{2n-2}^2),$$

$$(2n+1)!\, B_n = x\,(x^2+1^2)(x^2+3^2)\ldots(x^2+\overline{2n-1}^2),$$

avec

$$A_0 = 1 \qquad \text{et} \qquad B_0 = x,$$

on a les identités

$$A_n + \frac{1}{2} A_{n-1} + \frac{1.3}{2.4} A_{n-2} + \ldots = \frac{2n+1}{x} B_n,$$

$$B_n + \frac{1}{2} B_{n-1} + \frac{1.3}{2.4} B_{n-2} + \ldots = \frac{2n+2}{x} A_{n+1}.$$

Les trois exercices précédents sont dus à M. J.-W.-L. Glaisher.

106. Identités d'Euler. — Si l'on égale les coefficients de x^n dans les deux membres de l'identité (1) du numéro précédent, en observant que celui de X_k est 1, on obtient en supposant que le degré de $F(x)$ est au plus égal à n, et en désignant par M le coefficient de x^n dans $F(x)$,

$$M = \frac{F(x_0)}{A_0} + \frac{F(x_1)}{A_1} + \ldots + \frac{F(x_n)}{A_n}.$$

Remplaçons les quantités $x_0, x_1, \ldots, x_n$, par $a, b, c, \ldots, l$, et $F(x)$ par x^p, il en résulte que l'expression

$$\frac{a^p}{(a-b)(a-c)\ldots(a-l)} + \frac{b^p}{(b-a)(b-c)\ldots(b-l)} + \ldots$$

s'annule pour toutes les valeurs 0, 1, 2, ..., $(n-1)$ de p et devient égale à 1 pour $p = n$.

Exemple I. — Si $a, b, c, \ldots, l$ désignent les abscisses de $(n+1)$ points A, B, C, ..., L, en ligne droite sur l'axe OX, on a

$$OA = a, \quad OB = b, \quad AB = b - a;$$

par suite, l'expression

$$\frac{\overline{OA}^p}{AB.AC\ldots AL} + \frac{\overline{OB}^p}{BA.BC\ldots BL} + \ldots$$

s'annule ou est égale à $(-1)^n$ suivant que p est un entier non négatif plus petit que n, ou est égal à n. Ces formules ont été indiquées par Chasles, dans sa *Géométrie supérieure*. Par la méthode d'inversion, ou de transformation par rayons vecteurs réciproques, on généralise ces formules.

107. Sommation de fractions rationnelles. — Soit le polynôme

$$\varphi(x) = (x - x_0)(x - x_1)\ldots(x - x_n);$$

considérons une fraction rationnelle dans laquelle le degré du numérateur est au plus égal à $(n-1)$. Par la formule d'interpolation de Lagrange, on peut poser

$$\frac{f(x)}{\varphi(x)} = \frac{A_0}{x - x_0} + \frac{A_1}{x - x_1} + \ldots + \frac{A_n}{x - x_n},$$

$A_0, A_1, A_2, \ldots, A_n$, désignant des constantes. Si l'on fait

$$A_0 + A_1 + A_2 + \ldots + A_p = B_p,$$

on a identiquement

$$\frac{f(x)}{\varphi(x)} = B_0\left(\frac{1}{x-x_0} - \frac{1}{x-x_1}\right) + B_1\left(\frac{1}{x-x_1} - \frac{1}{x-x_2}\right)$$
$$+\ldots+B_{n-1}\left(\frac{1}{x-x_{n-1}} - \frac{1}{x-x_n}\right),$$

car B_n est nul, d'après l'une des identités d'Euler. Par conséquent, si les nombres $x_0, x_1, x_2, \ldots, x_n$, sont tous entiers, on pourra trouver la somme des valeurs de la fraction rationnelle donnée, pour des valeurs de x égales à une suite de nombres entiers consécutifs. Plus particulièrement, si $x_0, x_1, \ldots, x_n$ sont en progression arithmétique, on ramène le problème à la sommation des inverses des factorielles successives (n° 86).

Exemple I. — Trouver la somme S_n des n premiers termes de la suite

$$u_n = \frac{n(n+1)}{(n+2)(n+3)(n+4)(n+5)}.$$

On a l'identité

$$u_n = \frac{1}{3}\frac{1}{(n+2)(n+3)} - \frac{8}{3}\frac{1}{(n+3)(n+4)} + \frac{10}{3}\frac{1}{(n+4)(n+5)},$$

et l'on trouve

$$9S_n = (n+2)^2 u_n.$$

108. Formule d'interpolation de Newton. — Cette formule résout le problème de trouver le polynôme, de degré n au plus, qui pour des valeurs données de x, en nombre $(n+1)$,

$$x_0, \quad x_1, \quad x_2, \quad \ldots, \quad x_n,$$

supposées en progression arithmétique, prenne des valeurs données

$$u_0, \quad u_1, \quad u_2, \quad \ldots, \quad u_n.$$

En désignant par h la raison de la progression, ce polynôme a pour expression

$$u = u_0 + \frac{x-x_0}{h}\Delta u_0 + \frac{x-x_0}{h}\left(\frac{x-x_0}{h}-1\right)\frac{\Delta^2 u_0}{2!}+\ldots$$
$$+\frac{x-x_0}{h}\left(\frac{x-x_0}{h}-1\right)\cdots\left(\frac{x-x_0}{h}-n+1\right)\frac{\Delta^n u_0}{n!}.$$

En effet, si l'on désigne par p l'un des nombres $0, 1, 2, \ldots, n$, le premier membre devient u_p, lorsque l'on suppose dans le second

$$\frac{x-x_0}{h}=p \quad \text{ou} \quad x=x_p,$$

par suite de la formule fondamentale du calcul des différences

$$u_p=(1+\Delta)^p u_0.$$

Nous avons vu d'ailleurs qu'il n'existe qu'un seul polynôme de degré n, au plus (n° 73). Le problème revient encore à exprimer le polynôme cherché comme une fonction linéaire des polynômes

$$1, \quad \frac{x-x_0}{h}, \quad \frac{x-x_0}{h}\left(\frac{x-x_0}{h}-1\right), \quad \ldots,$$

dont les degrés représentent la suite complète des entiers de 0 à n. Lorsque les q derniers termes de la suite

$$u_0, \quad \Delta u_0, \quad \Delta^2 u_0, \quad \ldots, \quad \Delta^n u_0$$

s'annulent, le degré du polynôme u s'abaisse de q unités.

Inversement, si $f(x)$ est un polynôme de degré n, on a l'identité

$$f(x)=f(0)+\frac{x-x_0}{h}\frac{\Delta f(0)}{1!}+\frac{x-x_0}{h}\left(\frac{x-x_0}{h}-1\right)\frac{\Delta^2 f(0)}{2!}+\ldots.$$

109. Fonctions interpolaires d'Ampère. — Newton a étendu sa formule au cas où les valeurs données de la variable x ne sont plus en progression arithmétique (*Methodus differentialis*, 1711). Posons, par exemple, pour $n=3$,

$$u=\lambda_0+\lambda_1(x-x_0)+\lambda_2(x-x_0)(x-x_1)+\lambda_3(x-x_0)(x-x_1)(x-x_2).$$

En remplaçant successivement x par x_0, x_1, x_2, x_3, il vient

$$(1)\quad \begin{cases} u_0=\lambda_0,\\ u_1=\lambda_0+\lambda_1(x_1-x_0),\\ u_2=\lambda_0+\lambda_1(x_2-x_0)+\lambda_2(x_2-x_0)(x_2-x_1),\\ u_3=\lambda_0+\lambda_1(x_3-x_0)+\lambda_2(x_3-x_0)(x_3-x_1)+\lambda_3(x_3-x_0)(x_3-x_1)(x_3-x_2) \end{cases}$$

Si nous retranchons la première ligne des suivantes, si nous divisons respectivement par les différences

$$x_1 - x_0, \quad x_2 - x_0, \quad x_3 - x_0,$$

et si nous posons

$$\frac{u_1 - u_0}{x_1 - x_0} = v_1, \qquad \frac{u_2 - u_0}{x_2 - x_0} = v_2, \qquad \frac{u_3 - u_0}{x_3 - x_0} = v_3,$$

il vient le système

$$(2) \qquad \begin{cases} v_1 = \lambda_1, \\ v_2 = \lambda_1 + \lambda_2(x_2 - x_1), \\ v_3 = \lambda_1 + \lambda_2(x_3 - x_1) + \lambda_3(x_3 - x_1)(x_3 - x_2), \end{cases}$$

semblable au précédent, mais contenant une ligne en moins. En opérant de même et en posant

$$\frac{v_2 - v_1}{x_2 - x_1} = w_2, \qquad \frac{v_3 - v_1}{x_3 - x_1} = w_3,$$

on a le système

$$(3) \qquad \begin{cases} w_2 = \lambda_2, \\ w_3 = \lambda_2 + \lambda_3(x_3 - x_2); \end{cases}$$

donc, si l'on pose

$$\frac{w_3 - w_2}{x_3 - x_2} = s_3,$$

on trouve

$$\lambda_0 = u_0, \qquad \lambda_1 = v_1, \qquad \lambda_2 = w_2, \qquad \lambda_3 = s_3.$$

Cette méthode de calcul est assez rapide, en construisant un tableau analogue à celui des différences. Les expressions v, w, s, ... ont été appelées *fonctions interpolaires* par AMPÈRE. Il a observé que l'on a

$$v_1 = \frac{u_0}{x_0 - x_1} + \frac{u_1}{x_1 - x_0},$$

$$w_2 = \frac{u_0}{(x_0 - x_1)(x_0 - x_2)} + \frac{u_1}{(x_1 - x_0)(x_1 - x_2)} + \frac{u_2}{(x_2 - x_0)(x_2 - x_1)},$$

....;

ces formules, qu'il est facile d'établir d'une manière générale, permettent de déduire la formule d'interpolation de LAGRANGE de la seconde formule d'interpolation de NEWTON.

CHAPITRE XII.

LES POLYNOMES DÉRIVÉS.

---

110. Polynôme dérivé. — On appelle *polynôme dérivé* d'un polynôme entier

$$f(x) = Ax^n + Bx^{n-1} + \ldots + Kx + L,$$

le polynôme obtenu en multipliant chaque terme par l'exposant de x, et en diminuant de 1 l'exposant de x. On désigne le polynôme dérivé de $f(x)$ par $f'(x)$, et l'on a

$$f'(x) = nAx^{n-1} + (n-1)Bx^{n-2} + \ldots + K.$$

Soit, en particulier, le monôme Ax^n; on a, pour $x \gtrless a$, l'identité

$$\frac{Ax^n - Aa^n}{x-a} = A(x^{n-1} + ax^{n-2} + \ldots + a^{n-2}x + a^{n-1});$$

pour $x = a$, le premier membre se présente sous une forme indéterminée, tandis que le second membre devient nAa^{n-1}, et l'on dit que cette expression est la valeur du premier membre pour $x = a$. Plus généralement, la fraction

$$\frac{f(x) - f(a)}{x-a} = A\frac{x^n - a^n}{x-a} + B\frac{x^{n-1} - a^{n-1}}{x-a} + \ldots + K\frac{x-a}{x-a},$$

toujours égale à un certain polynôme contenant x et a, pour $x \gtrless a$, se présente, pour $x = a$, sous la forme $\frac{0}{0}$, et l'on dit que le second membre représente la valeur du premier, même pour la valeur exceptionnelle $x = a$. C'est précisément la valeur de l'expression $f'(a)$, obtenue en remplaçant x par a dans le polynôme dérivé.

Le polynôme dérivé, ou la *dérivée* d'un polynôme $f(x)$ de degré n, est un polynôme de degré $(n-1)$ dont on peut prendre

aussi la dérivée, que l'on appelle *dérivée seconde;* on la désigne par $f''(x)$: c'est un polynôme de degré $(n-2)$. En général, la dérivée $p^{\text{ième}}$ d'un polynôme $f(x)$, de degré n, est un polynôme de degré $(n-p)$; la dérivée $n^{\text{ième}}$ se réduit à la constante $n!A$, et les dérivées d'ordre plus élevé sont nulles. On désigne la dérivée d'ordre p de $f(x)$ par l'une des notations

$$\frac{d^p f(x)}{dx^p}, \quad f^{(p)}(x), \quad D^p f(x),$$

employées respectivement par LEIBNIZ, LAGRANGE et CAUCHY. Nous nous servirons, suivant les cas, de la notation la plus commode.

Il résulte immédiatement de la définition que la dérivée $p^{\text{ième}}$ d'une somme algébrique de polynômes égale la somme des dérivées $p^{\text{ièmes}}$ des termes de cette somme; ainsi

$$D^p[a f(x) + b\varphi(x) + c\psi(x)] = a D^p f(x) + b D^p \varphi(x) + c D^p \psi(x).$$

111. Dérivées d'un produit et d'un quotient. — Si l'on désigne par y le produit de deux polynômes u et v contenant la variable x, et si l'on donne à x l'accroissement Δx, il en résulte pour u, v, y les accroissements Δu, Δv, Δy: on a

$$\Delta y = (u + \Delta u)(v + \Delta v) - uv;$$

puis

$$\frac{\Delta y}{\Delta x} = u\frac{\Delta v}{\Delta x} + v\frac{\Delta u}{\Delta x} + \frac{\Delta u}{\Delta x}\Delta v;$$

et, pour $\Delta x = 0$,

$$y' = uv' + vu'.$$

En divisant par uv, on peut écrire

$$\frac{y'}{y} = \frac{u'}{u} + \frac{v'}{v};$$

l'expression $\frac{y'}{y}$ s'appelle la dérivée logarithmique du polynôme y. Par suite : *La dérivée logarithmique d'un produit est égale à la somme des dérivées logarithmiques des facteurs.*

Ce théorème s'étend à un nombre quelconque de facteurs. Par suite, la dérivée d'un produit de plusieurs facteurs égale la somme

des résultats obtenus en multipliant la dérivée de chacun des facteurs par le produit de tous les autres.

Si l'on a $y = (u : v)$, on obtient

$$\Delta y = \frac{u + \Delta u}{v + \Delta v} - \frac{u}{v},$$

$$\frac{\Delta y}{\Delta x} = \frac{v\Delta u - u\Delta v}{\Delta x}\,\frac{1}{v(v + \Delta v)},$$

et enfin

$$y' = \frac{vu' - uv'}{v^2}.$$

En particulier, la dérivée de $\frac{1}{x^m}$ ou de x^{-m}, pour m entier, est $(-m)x^{(-m)-1}$; ainsi la dérivée de x^m est mx^{m-1} pour m entier négatif, comme pour m entier positif.

La dérivée logarithmique d'un quotient est égale à la différence des dérivées logarithmiques du dividende et du diviseur.

Exemple I. — Soit

$$y = u^\alpha v^\beta w^\gamma \ldots,$$

en désignant par α, β, γ, ... des entiers positifs ou négatifs, on a

$$\frac{y'}{y} = \alpha\frac{u'}{u} + \beta\frac{v'}{v} + \gamma\frac{w'}{w} + \ldots.$$

Enfin supposons que y soit une *fonction de fonctions*, c'est-à-dire que y soit exprimée en fonction de x par des variables intermédiaires

$$y = \psi(v), \qquad v = \varphi(u), \qquad u = f(x),$$

de telle sorte que $y = F(x)$. On peut trouver la dérivée y' sans qu'il soit nécessaire de faire les substitutions; en effet,

$$\frac{\Delta y}{\Delta x} = \frac{\Delta y}{\Delta v}\,\frac{\Delta v}{\Delta u}\,\frac{\Delta u}{\Delta x},$$

et, par suite,

$$y' = \psi'(v)\,\varphi'(u)\,f'(x).$$

112. Formule de Taylor. — Ce théorème a pour but d'exprimer un polynôme $f(x+h)$ en fonction linéaire de $f(x)$ et de ses polynômes dérivés $f'(x)$, $f''(x)$, ... (n° 102). Ce n'est ainsi que la formule du binôme de Newton, avec un changement de

notation, lorsqu'il ne s'agit que des fonctions entières. On a, en effet,

$$(x+h)^n = x^n + \frac{h}{1!} n x^{n-1} + \frac{h^2}{2!} n(n-1)x^{n-2} + \ldots$$
$$+ \frac{h^p}{p!} n(n-1)\ldots(n-p+1)x^{n-p} + \ldots + \frac{h^n}{n!} n!$$

et, en posant $f(x) = \mathrm{A}x^n$, il vient

$$(1)\quad f(x+h) = f(x) + \frac{h}{1!} f'(x) + \ldots + \frac{h^p}{p!} f^{(p)}(x) + \ldots + \frac{h^n}{n!} f^{(n)}(x).$$

Pour d'autres monômes, $\mathrm{B}x^r$, $\mathrm{C}x^s$, ..., on a des formules analogues; donc, si l'on fait la somme des développements obtenus, en tenant compte du théorème sur la dérivée d'une somme, on en déduit que le développement (1) subsiste pour un polynôme de degré quelconque.

Cette formule donne encore le développement de

$$(2)\qquad \Delta f(x) = f(x+h) - f(x),$$

c'est-à-dire de la différence d'un polynôme $f(x)$, ordonné suivant les puissances de l'accroissement h de la variable.

Si l'on fait $x = 0$, et si l'on remplace ensuite h par x, on obtient la formule de Mac Laurin

$$(3)\qquad f(x) = f(0) + \frac{x}{1!} f'(0) + \frac{x^2}{2!} f''(0) + \ldots + \frac{x^n}{n!} f^{(n)}(0).$$

Enfin, si l'on suppose $h = -x$, on a la formule de Bernoulli (¹)

$$(4)\qquad f(0) = f(x) - \frac{x}{1!} f'(x) + \frac{x^2}{2!} f''(x) - \ldots + \frac{(-x)^n}{n!} f^{(n)}(x).$$

113. Facteurs multiples d'un polynôme. — On dit que le polynôme $f(x)$ contient le facteur $(x-a)$ au degré de multiplicité p, lorsque $f(x)$ est égal au produit de $(x-a)^p$ par un polynôme $\varphi(x)$ qui n'est pas divisible par $(x-a)$, de telle sorte que l'on a

$$f(x) = (x-a)^p\, \varphi(x),$$

avec l'hypothèse $\varphi(a) \gtrless 0$. On a le théorème suivant : *Pour que*

(¹) Cette formule a été publiée avant celle de Taylor.

le polynôme $f(x)$ soit divisible par $(x-a)^p$, il faut et il suffit que le polynôme $f(x)$ et ses $(p-1)$ premières dérivées s'annulent pour $x = a$.

En effet, si l'on remplace, dans la formule de Taylor, x par a et h par $(x-a)$, il vient

$$(1)\quad f(x) = f(a) + \frac{x-a}{1!} f'(a) + \ldots + \frac{(x-a)^{p-1}}{(p-1)!} f^{(p-1)}(a) + \ldots;$$

par suite, *le quotient de $f(x)$ par $(x-a)^p$ est le polynôme*

$$\frac{1}{p!} f^{(p)}(a) + \frac{x-a}{(p+1)!} f^{(p+1)}(a) + \ldots + \frac{(x-a)^{n-p}}{n!} f^{(n)}(a),$$

et le reste de la division de $f(x)$ par $(x-a)^p$ est le polynôme

$$f(a) + \frac{x-a}{1!} f'(a) + \frac{(x-a)^2}{2!} f''(a) + \ldots + \frac{(x-a)^{p-1}}{(p-1)!} f^{(p-1)}(a).$$

Ainsi, pour que $f(x)$ soit divisible par $(x-a)^p$, il faut et il suffit que le reste de la division soit nul, quelle que soit la valeur de x et, par suite, quelle que soit la valeur de $(x-a)$; on a donc les p conditions

$$[illegible] \quad f^{(p-1)}(a) = 0;$$

réciproquement, si ces p conditions sont vérifiées et si $f^{(p)}(a)$ n'est pas nul, le polynôme $f(x)$ est divisible par $(x-a)^p$, et non [illegible]

116. Règle de L'Hospital. — Lorsque les deux termes d'un [illegible] même valeur a de x, l[illegible] remplac[illegible] conformément à la for[illegible] la règle suivante [illegible] jusqu'à c[illegible] ne s'annulen[illegible] rappor[illegible] limite, si p es[illegible]

on a, en prenant la dérivée et en multipliant par x,

$$xf'_p = f_{p+1};$$

mais, pour $p = 0$,

$$f_0 = x + x^2 + \ldots + x^{n-1},$$

ou bien

$$f_0 = \frac{x - x^n}{1 - x};$$

on a donc successivement

$$f_1 = x\,\mathrm{D}\,\frac{x - x^n}{1 - x},$$

$$f_2 = x\,\mathrm{D}\left(x\,\mathrm{D}\,\frac{x - x^n}{1 - x}\right),$$

$$f_3 = x\,\mathrm{D}\left[x\,\mathrm{D}\left(x\,\mathrm{D}\,\frac{x - x^n}{1 - x}\right)\right],$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

et ainsi de suite.

Si l'on fait $x = 1$, les valeurs de $f_1, f_2, f_3, \ldots$ se présentent sous une forme indéterminée ; mais, en appliquant la règle de L'Hospital, on trouve ainsi, par un procédé détourné, la somme des carrés, des cubes, des bicarrés, ..., des $(x - 1)$ premiers entiers (Abel, *Œuvres complètes*, 2e édition, t. II, p. 14).

Exemple II. — La dérivée d'ordre p de

$$g(x) = \frac{x^{n+p-1} - 1}{x - 1}$$

a pour développement

$$1.2\ldots p + 2.3\ldots(p+1)x + \ldots + n(n+1)\ldots(n+p-1)x^{n-1};$$

en formant directement $g'(x)$, $g''(x)$, $g'''(x)$, ... et faisant ensuite $x = 1$, on retrouve la sommation des factorielles consécutives (n° 37).

115. Formule d'Abel. — Nous avons vu que si $f(x)$ désigne un polynôme de degré n, et $\varphi_0, \varphi_1, \varphi_2, \ldots, \varphi_n$ des polynômes donnés dont les degrés reproduisent la suite des nombres entiers, le polynôme $f(x)$ peut être développé suivant la forme linéaire

$$f(x) = \lambda_0\varphi_0 + \lambda_1\varphi_1 + \lambda_2\varphi_2 + \ldots + \lambda_n\varphi_n,$$

les coefficients λ étant indépendants de x. Désignons par β une constante quelconque, et posons

$$\varphi_0 = 1, \quad \varphi_1(x) = x, \quad \varphi_2(x) = \frac{x(x - 2\beta)}{2!}, \quad \ldots,$$

$$\varphi_p(x) = \frac{x(x - p\beta)^{p-1}}{p!}.$$

des lettres qui représentent les variables. Le polynôme peut avoir des degrés différents par rapport à chacune des variables; on appelle *degré* d'un terme le nombre égal à la somme des exposants des variables qu'il contient, et le degré du polynôme est égal au degré du terme du plus haut degré.

On peut prendre les dérivées du polynôme par rapport à chacune des variables, et les dérivées successives par rapport à des variables différentes. Les *dérivées partielles* du premier ordre de $f(x, y, z)$, prises par rapport à y, par exemple, se désignent par l'une des notations

$$f'_y(x, y, z), \quad \frac{\partial f(x, y, z)}{\partial y}, \quad D_y f(x, y, z);$$

lorsque l'on donne ensuite à x, y, z certaines valeurs x_0, y_0, z_0, il suffit, pour indiquer cette opération, de remplacer, dans les parenthèses, x, y, z respectivement par x_0, y_0, z_0.

Si l'on prend la dérivée du terme

$$T = N x^a y^b z^c$$

α fois par rapport à x, puis β fois par rapport à y, puis γ fois par rapport à z, on obtient, en désignant par la lettre A les arrangements simples (nº 15),

$$N A_a^\alpha A_b^\beta A_c^\gamma x^{a-\alpha} y^{b-\beta} z^{c-\gamma};$$

le résultat est indépendant de l'ordre des dérivations. Pour toute fonction entière f, il en est de même; le résultat s'indique par l'une des notations

$$f^{(\alpha+\beta+\gamma)}_{x^\alpha y^\beta z^\gamma}(x, y, z), \quad \frac{\partial^{\alpha+\beta+\gamma} f(x, y, z)}{\partial x^\alpha \partial y^\beta \partial z^\gamma}, \quad D_{x^\alpha y^\beta z^\gamma} f(x, y, z).$$

118. Formule de Taylor pour une fonction de plusieurs variables. — Soit une fonction $f(x, y, z)$ de trois variables, par exemple; il s'agit de développer l'expression

$$f(x + h, y + k, z + l)$$

suivant les puissances des accroissements h, k, l des variables x, y, z. Pour simplifier, nous nous servirons d'un symbole d'opération Θ, qui désigne le résultat que l'on obtient en faisant la

somme des dérivées partielles f'_x, f'_y, f'_z de $f(x, y, z)$, multipliées respectivement par les accroissements h, k, l. Ainsi, par définition,

$$\theta f = hf'_x + kf'_y + lf'_z.$$

Mais θf est un polynôme en x, y, z, sur lequel on peut répéter la même opération dont nous désignons le résultat par $\theta^2 f$, et ainsi de suite. On a, en général,

$$\theta^{p+q} f = \theta^p.\theta^q f = \theta^q.\theta^p f.$$

Appliquons l'opération θ aux dérivées partielles de $f(x, y, z)$,

$$\begin{aligned} \theta f'_x &= hf''_{xx} + kf''_{xy} + lf''_{xz}, \\ \theta f'_y &= hf''_{yx} + kf''_{yy} + lf''_{yz}, \\ \theta f''_z &= hf''_{zx} - kf''_{zy} + lf''_{zz}. \end{aligned}$$

Si l'on multiplie respectivement ces trois égalités par h, k, l et si l'on ajoute les résultats, il vient, en tenant compte du théorème sur l'interversion de l'ordre des dérivations (n° **117**),

$$\theta^2 f = h^2 f''_{xx} + \ldots + 2klf''_{yz} + \ldots,$$

ou, sous la forme symbolique,

$$\theta^2 f \triangleq \left(h \frac{\partial}{\partial x} + k \frac{\partial}{\partial y} + l \frac{\partial}{\partial z}\right)^2 f,$$

en y considérant $\frac{\partial}{\partial x}$, $\frac{\partial}{\partial y}$, $\frac{\partial}{\partial z}$ comme des quantités, et à la condition de remplacer, après le développement du second membre, leurs exposants par des indices de dérivation.

Le symbole θ est *distributif,* comme celui de la dérivée D_x ou $\frac{\partial}{\partial x}$, c'est-à-dire que, si l'on considère plusieurs fonctions f, φ, ψ des variables x, y, z, on a, quelles que soient les constantes A, B, C,

$$\theta(Af + B\varphi + C\psi) = A\theta f + B\theta\varphi + C\theta\psi.$$

Cela posé, la formule de Taylor, étendue à un polynôme de plusieurs variables, s'écrit

$$(1) \qquad f(x+h, y+k, z+l) = f + \frac{1}{1!}\theta f + \frac{1}{2!}\theta^2 f + \frac{1}{3!}\theta^3 f + \ldots.$$

Pour vérifier l'exactitude de cette formule, il suffit de considérer la fonction

$$f(x,y,z) = x^a y^b z^c.$$

Le coefficient de $h^\alpha k^\beta l^\gamma$ dans le développement de

$$(x+h)^a (y+k)^b (z+l)^c$$

est, en se servant de la notation des arrangements simples (n° 45)

$$(2) \qquad \frac{A_a^\alpha}{\alpha!} x^{a-\alpha} \cdot \frac{A_b^\beta}{\beta!} x^{b-\beta} \cdot \frac{A_c^\gamma}{\gamma!} x^{c-\gamma}.$$

D'autre part, si l'on suppose

$$n = \alpha + \beta + \gamma,$$

le coefficient de $h^\alpha k^\beta l^\gamma$ dans

$$\frac{1}{n!} \Theta^n f = \frac{1}{n!} \left(h \frac{\partial}{\partial x} + k \frac{\partial}{\partial y} + l \frac{\partial}{\partial z} \right)^n f$$

est, d'après le n° 80, égal à

$$\frac{1}{n!} \frac{n!}{\alpha!\,\beta!\,\gamma!} \frac{\partial^n f}{\partial x^\alpha \partial y^\beta \partial z^\gamma},$$

ou

$$\frac{1}{\alpha!\,\beta!\,\gamma!} A_a^\alpha x^{a-\alpha} . A_b^\beta y^{b-\beta} . A_c^\gamma z^{c-\gamma},$$

qui ne diffère pas de l'expression (2).

119. Fonctions homogènes. — Un polynôme entier en x, y, z est homogène et de degré n lorsque tous ses termes sont de même degré n; par suite, quelle que soit la valeur de t, on a l'identité

$$f(tx, ty, tz) = t^n f(x, y, z).$$

La somme algébrique de fonctions homogènes de même degré est une fonction homogène de même degré.

Le produit ou le quotient de deux fonctions homogènes de degrés p et q est une fonction homogène de degré $(p \pm q.)$

Toute fonction homogène, de degré n, des variables x, y, z est

égale au produit de la puissance $n^{\text{ième}}$ de l'une d'elles par une fonction des rapports des autres variables à celle-ci, et inversement.

Les formules de la Géométrie sont homogènes.

Les dérivées d'ordre p d'une fonction homogène de degré n sont des fonctions homogènes de degré $(n-p)$.

120. Théorème d'Euler. — Toute fonction homogène, et de degré n, des variables x, y, z vérifie l'identité

$$x\frac{\partial f}{\partial x}+y\frac{\partial f}{\partial y}+z\frac{\partial f}{\partial z}=nf(x,y,z);$$

on a de même

$$x^2\frac{\partial^2 f}{\partial x^2}+\ldots+2yz\frac{\partial^2 f}{\partial y\,\partial z}+\ldots=n(n-1)f(x,y,z),$$

et, en général, avec la notation du n° 118,

$$\theta^p f(x,y,z)\doteq n(n-1)\ldots(n-p+1)f(x,y,z),$$

après avoir remplacé, dans le développement du premier membre, les exposants de $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}$, par des indices de dérivation, et h, k, l par x, y, z.

L'emploi des formules d'Euler permet de transformer des relations en d'autres plus simples, en rendant homogènes des polynômes qui ne le sont pas, par l'introduction d'une nouvelle lettre que l'on considère comme une variable arbitraire, et que l'on remplace ensuite par 1.

Soit, par exemple, le polynôme $f(x)$, de degré n, que l'on peut écrire sous la forme homogène

$$y^n f\left(\frac{x}{y}\right) \quad \text{ou} \quad f(x,y).$$

Pour que ce polynôme soit divisible par $(x-ay)^p$, il faut et il suffit (n° 113) qu'en remplaçant x par a, et y par 1, dans la suite des dérivées

$$f(a,1),\; f'_x(a,1),\; f''_{x^2}(a,1),\; \ldots,\; f^{(p-1)}_{x^{p-1}}(a,1),$$

tous les résultats soient nuls. Par les formules d'Euler, on substitue à ces conditions les conditions équivalentes

$$\frac{\partial^{p-1} f(a, 1)}{\partial x^{p-1}} = 0, \qquad \frac{\partial^{p-1} f(a, 1)}{\partial x^{p-2}\,\partial y} = 0, \qquad \dots \qquad \frac{\partial^{p-1} f(a, 1)}{\partial y^{p-1}} = 0;$$

en d'autres termes, il faut et il suffit que les p dérivées partielles de l'ordre $(p-1)$, prises par rapport à x et y, s'annulent lorsque l'on y remplace x par a et y par 1.

Exemple I. — Si $f(x, y, z, \dots)$ est un polynôme homogène de degré n, on a l'identité

$$\frac{1}{q!}\left(x_1\frac{\partial}{\partial x}+\dots\right)^q f(x_0, y_0, \dots) = \frac{1}{(n-q)!}\left(x_0\frac{\partial}{\partial x_1}+\dots\right)^{n-q} f(x_1, y_1, \dots).$$

CHAPITRE XIII.

LE CALCUL SYMBOLIQUE.

On doit considérer le calcul symbolique comme une méthode rapide pour l'écriture des formules dans une suite de déductions théoriques; mais, lorsqu'il s'agit de déterminer les valeurs des nombres fournis par ce calcul, il est indispensable de remplacer la formule symbolique par le développement ordinaire. On fait de même lorsque la suite des raisonnements laisse dans l'esprit une certaine obscurité; alors on remplace encore la formule par les notations ordinaires. C'est donc, en quelque sorte, pour le développement des nouvelles théories, une sténographie des formules de l'Arithmétique et de l'Algèbre.

Cette méthode est déjà ancienne; on la trouve comme procédé mnémonique dans les écrits de Leibniz, pour les dérivées successives d'un produit de deux ou de plusieurs facteurs; on la retrouve dans la série de Taylor étendue au cas de plusieurs variables; nous l'avons déjà employée dans les formules fondamentales du calcul des différences. Développée plus tard par Laplace, par Vandermonde et par Herschel, elle a été considérablement augmentée par les travaux de Cayley et de Sylvester, dans la théorie des formes.

Dans un ouvrage intitulé *Calculus of Operations*, Carmichael a exposé les méthodes générales de ce calcul rapide; ses développements se rapportent surtout à l'emploi des symboles d'opération, comme ceux du calcul des sommes et des différences Σ et Δ, et ceux du Calcul différentiel et du Calcul intégral. Mais la méthode symbolique, que nous employons ici, diffère des précédentes sous ce rapport, que les symboles que nous considérons désignent des quantités et non des opérations; nous nous rapprochons ainsi pour une partie de la notation, employée par Cayley, pour les polynômes entiers (*quantics*). L'application de cette méthode nous a permis de simplifier, d'une manière très notable, les raisonnements et les

résultats sur le calcul des sommes et des différences, sur les nombres de Bernoulli et d'Euler, sur la théorie des séries récurrentes et, par suite, sur la théorie générale des fonctions. Par notre méthode, les développements prennent une forme plus concise, plus condensée, qui conduit à des généralisations successives et indéfinies des propriétés qui concernent les nombres, et des formules qui les renferment. Ainsi, dit Laplace, « la langue de l'analyse, la plus parfaite de toutes, étant par elle-même un puissant instrument de découvertes, ses notations, lorsqu'elles sont nécessaires et heureusement imaginées, sont les germes de nouveaux calculs. »

Ce Chapitre contient quelques principes généraux, et leur application à la solution de plusieurs problèmes considérés par Euler. Ceux-ci se rapportent aux Permutations figurées et à l'Arithmétique de position ; le Chapitre suivant donne l'application du calcul symbolique au Calcul des sommes et au Calcul des différences.

121. **Du symbole potentiel.** — Considérons des nombres quelconques

$$(b) \qquad b_0,\ b_1,\ b_2,\ \ldots,\ b_p,\ \ldots,$$

formant une suite limitée ou illimitée, de telle sorte qu'à chaque valeur de l'indice corresponde un nombre déterminé.

Nous désignerons par b le symbole des nombres de cette suite, et nous supposerons que, dans les formules transitoires, b est une quantité assujettie aux lois ordinaires du calcul algébrique et, en particulier, à la règle des exposants entiers et positifs,

$$b^m . b^n \triangleq b^{m+n}.$$

A la fin des calculs, on doit remplacer les exposants de b par des indices et les nombres b par ceux de la suite.

Soit un polynôme de degré n, dans lequel nous mettons en évidence les coefficients du développement de $(1 + x)^n$,

$$f(x) = b_0 x^n + \frac{n}{1} b_1 x^{n-1} + \frac{n(n-1)}{1.2} b_2 x^{n-2} + \ldots + b_n x^0;$$

nous pouvons écrire ce polynôme sous la forme condensée

$$f(x) \triangleq (x + b)^n,$$

en ayant toujours le soin de *tenir compte de l'exposant zéro* de b et du nombre correspondant b_0.

On voit immédiatement que la dérivée $f'(x)$ du polynôme $f(x)$ peut s'écrire symboliquement

$$f'(x) \doteq n(x+b)^{n-1},$$

et, par suite, on a pour la dérivée d'ordre p,

$$f^{(p)}(x) \doteq n(n-1)\ldots(n-p+1)(x+b)^{n-p}.$$

Exemple I. — Si l'on suppose

$$u \doteq (x+a)^n, \qquad v \doteq (x+b)^n,$$

et si l'on considère l'expression

$$y = uv^n - u'v^{n-1} + u''v^{n-2} + \ldots + (-1)^n u^n v,$$

dans laquelle les exposants sont des indices de dérivation, la fonction y est indépendante de x. (HALPHEN).

On voit, en effet, que la dérivée y' est nulle; on obtient la valeur de y, en remplaçant x par o, ce qui donne

$$y \doteq n!(a-b)^n.$$

Plus généralement, considérons le polynôme homogène

$$f(x,y) = b_0 a_n x^n y^0 + \frac{n}{1} b_1 a_{n-1} x^{n-1} y + \frac{n(n-1)}{1.2} b_2 a_{n-2} x^{n-2} y^2 + \ldots + b_n a_0 x^0 y^n;$$

nous pouvons l'écrire sous la forme symbolique condensée

$$f(x,y) \doteq (ax+by)^n,$$

en supposant que l'on remplace, après le développement du second membre, les exposants de a et de b par des indices. On trouve, comme précédemment,

$$\frac{\partial f}{\partial x} \doteq na(ax+by)^{n-1},$$

$$\frac{\partial f}{\partial y} \doteq nb(ax+by)^{n-1}.$$

On peut donc appliquer à un polynôme symbolique les procédés

ordinaires de dérivation ; d'ailleurs, on peut considérer des polynômes contenant un nombre quelconque de variables et de symboles, tels que

$$(ax + by + cz + \dots)^n.$$

Lorsqu'un polynôme $f(x)$, à une seule variable, n'est pas homogène, on peut toujours l'écrire sous la forme homogène $f(x, y)$; il suffit, dans les résultats, de remplacer ensuite y par 1 ; cette remarque s'applique d'ailleurs aux polynômes contenant un nombre quelconque de variables. Ainsi les propriétés des formes homogènes s'appliquent aux polynômes symboliques.

Nous avons supposé que l'on peut représenter par une lettre le symbole d'une suite de quantités données ; inversement, on peut calculer successivement les termes d'une suite définie par un symbole. Soit, par exemple, une suite donnée

$$(a) \qquad a_0, a_1, a_2, \dots, a_n, \dots ;$$

on peut, de bien des manières différentes, calculer des suites de nombres qui dépendent des nombres de la suite (a).

Posons, par exemple,

$$(1) \qquad b_n \doteq (a + 1)^n,$$

c'est-à-dire

$$b_n = a_n + \frac{n}{1} a_{n-1} + \frac{n(n-1)}{1.2} a_{n-2} + \dots + a_0 ;$$

Nous allons montrer que l'on peut introduire, dans la relation (1), une variable quelconque z ; en effet, soit $f(x)$ un polynôme quelconque

$$f(x) = p_0 x^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots + p_n x^0 ;$$

nous avons, d'après la formule (1),

$$\begin{aligned}
b_n &\doteq (a + 1)^n, \\
b_{n-1} &\doteq (a + 1)^{n-1}, \\
&\dots\dots\dots\dots\dots\dots, \\
&\dots\dots\dots\dots\dots\dots, \\
b_2 &\doteq (a + 1)^2, \\
b_1 &\doteq (a + 1)^1, \\
b_0 &\doteq a_0,
\end{aligned}$$

En multipliant respectivement ces égalités par $p_0, p_1, p_2, \ldots, p_n$ et en ajoutant, il vient

$$(2)\qquad f(b) \triangleq f(a+1).$$

Cette relation subsiste, quelle que soit la fonction entière $f(x)$. Nous pouvons donc écrire les égalités

$$\begin{array}{l} f(b) \triangleq f(a+1), \\ f'(b) \triangleq f'(a+1), \\ f''(b) \triangleq f''(a+1), \\ \ldots\ldots\ldots\ldots\ldots, \\ \ldots\ldots\ldots\ldots\ldots; \end{array}$$

en les multipliant respectivement par

$$1, \quad \frac{z}{1!}, \quad \frac{z^2}{2!}, \quad \frac{z^3}{3!}, \quad \ldots, \quad \frac{z^n}{n!},$$

il vient, en ajoutant et en tenant compte de la formule de Taylor, l'égalité symbolique

$$f(z+b) \triangleq f(z+a+1).$$

Ce procédé d'extension d'une égalité symbolique s'applique évidemment à une fonction d'un nombre quelconque de variables et de symboles. Ainsi, dans la formule précédente, on pourra supposer que z représente un symbole au lieu d'un nombre.

Non seulement les formules symboliques déterminent des nombres par des relations avec des nombres donnés à l'avance, mais elles peuvent servir à déterminer les termes successifs d'une suite inconnue. Ainsi, par exemple, la formule

$$(B+1)^n - B^n \triangleq 0,$$

pour $n > 1$, en supposant $B_0 = 1$, $B_1 = -\frac{1}{2}$, permet de déterminer successivement des nombres B_2, B_3, B_4, ..., et ainsi indéfiniment; nous verrons plus loin que ces nombres sont fort importants dans les développements de l'Arithmétique et de l'Algèbre; on les appelle *nombres de* Bernoulli. Nous devons ajouter que, pour la simplification des raisonnements et des formules, il nous a paru indispensable de modifier légèrement les notations ordinaires de ces nombres.

122. Du symbole exponentiel. — Au lieu de mettre en évidence, dans le développement de $f(x)$, les coefficients du binôme, on peut y mettre telle suite régulière ou irrégulière de coefficients donnés à l'avance; ainsi, par exemple, nous pouvons toujours écrire un polynôme $f(x)$, de degré n, sous la forme

$$f(x) = a_0 + \frac{a_1}{1!}x + \frac{a_2}{2!}x^2 + \frac{a_3}{3!}x^3 + \ldots + \frac{a_n}{n!}x^n.$$

Nous désignerons ce polynôme par la notation condensée $\exp ax$, que nous appellerons la *forme symbolique exponentielle.* Nous allons d'abord donner les dérivées successives d'un polynôme écrit sous cette forme. Soit donc

$$f(x) \doteq \exp ax.$$

En supposant le polynôme développé et en prenant la dérivée, on vérifie immédiatement que l'on a

$$f'(x) \doteq a \exp ax,$$
$$f''(x) \doteq a^2 \exp ax,$$

et, en général,

$$f^{(p)}x \doteq a^p \exp ax.$$

Le développement de la puissance d'un binôme peut s'écrire sous la forme exponentielle; ainsi, si l'on désigne par p_n le nombre des arrangements simples de p lettres prises n à n, c'est-à-dire si l'on pose

$$p_n = p(p-1)\ldots(p-n+1),$$

on a la formule

$$(1+x)^p \doteq \exp px;$$

on a, de même, pour d'autres valeurs de l'exposant,

$$(1+x)^q \doteq \exp qx;$$
$$(1+x)^r \doteq \exp rx;$$

supposons $r = p + q$; la formule du binôme de Vandermonde peut s'écrire sous la forme condensée

$$(1) \qquad r_n \doteq (p+q)^n;$$

et, par suite,

$$(2) \qquad \exp px \times \exp qx \doteq \exp(p+q)x.$$

D'ailleurs, puisque les développements des binômes de NEWTON et de VANDERMONDE ne reposent que sur la règle des exposants, à savoir

$$p^m . p^n = p^{m+n},$$

il en résulte que l'identité (2) subsiste pour deux polynômes exponentiels quelconques, $\exp px$ et $\exp qx$, et que le produit de ceux-ci est un polynôme exponentiel, $\exp rx$, dont les coefficients se déterminent par la formule (1).

Le théorème précédent s'applique au produit d'un nombre quelconque de polynômes exponentiels, et ainsi

$$\exp(ax).\exp(bx).\exp(cx) \triangleq \exp(a+b+c)x,$$
$$\exp ax . \exp bx . \exp cx . \exp dx \triangleq \exp(a+b-c+d)x.$$

Cependant, on doit observer que, si deux polynômes deviennent identiques, on n'a pas le droit d'écrire

$$(\exp ax)^2 \triangleq \exp 2ax;$$

mais il faut calculer les coefficients b du carré de la forme $\exp ax$, par la relation

$$b^n \triangleq (a + a')^n,$$

en considérant d'abord comme distincts a et a', et en remplaçant ensuite, dans le résultat final, a^n et a'^n par a_n.

123. Problème des rencontres. — Nous appliquerons les méthodes du calcul symbolique à plusieurs problèmes sur les permutations et, en particulier, au célèbre problème du chevalier de MONTMORT, traité par EULER, et connu sous le nom de *problème des rencontres*. Il s'agit de déterminer le nombre des permutations de n éléments

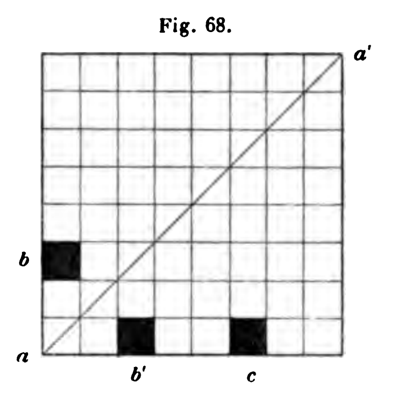
$$a_1, \quad a_2, \quad \ldots, \quad a_n,$$

dans lesquelles aucun élément n'est placé à un rang égal à son indice. Ce problème revient évidemment à déterminer le nombre des permutations figurées (problème des tours, n° 43), dans lesquelles il ne se trouve aucun élément sur l'une des diagonales, telle que aa' (*fig.* 68).

Désignons par Q_n le nombre des permutations dans lesquelles

aucun élément n'est à son rang naturel, et par P_n le nombre total $n!$ des permutations. Soit b l'une des $(n-1)$ positions de la tour, sur la première colonne, la case a du coin étant exceptée, d'après l'hypothèse. Nous devons considérer deux cas, suivant que, dans la ligne inférieure, il y a une tour b' symétrique de b par rapport à la diagonale aa', ou en une autre position quelconque c. Dans le premier cas, en supprimant les lignes et les colonnes con-

Fig. 68.



Problème des rencontres.

tenant b et b', il reste un ensemble de cases qui correspond, dans la question présente, à un échiquier de $(n-2)$ cases de côté. Dans le second cas, échangeons les colonnes contenant b et c; alors c vient en a, et b sur une case non située sur la diagonale; par suite, en supprimant la première ligne et la première colonne, il reste une solution sur l'échiquier de $(n-1)$ cases de côté; on a donc la relation de récurrence

$$(1) \qquad Q_n = (n-1)[Q_{n-1} + Q_{n-2}].$$

On trouve ainsi successivement, pour les premières valeurs de n,

n	0,	1,	2,	3,	4,	5,	6,	7,	8,
Q_n	1,	0,	1,	2,	9,	44,	265,	1854,	14833.

On observe immédiatement, pour les premières valeurs de n, en divisant chaque nombre Q par le précédent, la loi suivante

$$(2) \qquad Q_n = nQ_{n-1} + (-1)^n;$$

nous allons démontrer que cette relation est générale. En effet, si dans la relation (1) nous changeons n en $(n+1)$, il vient

$$Q_{n+1} = n(Q_n + Q_{n-1});$$

en retranchant de la précédente, on trouve

$$Q_{n+1} = (n+1)Q_n + (-1)^{n+1};$$

c'est précisément la relation (2), dans laquelle on remplace n par $(n+1)$. Ainsi, cette formule est générale. En divisant ses deux membres par $P_n = n!$, nous avons

$$\frac{Q_n}{P_n} = \frac{Q_{n-1}}{P_{n-1}} + \frac{(-1)^n}{P_n};$$

si l'on fait successivement $n = 2, 3, 4, \ldots$, et si l'on ajoute les égalités obtenues, il vient

$$\frac{Q_n}{P_n} = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \ldots + \frac{(-1)^n}{n!}.$$

La méthode précédente ne diffère de la solution donnée par Euler que par la forme géométrique (¹). Nous exposerons une autre méthode fondée sur le calcul symbolique; cette solution, très remarquable par son élégante simplicité, est due à M. Neuberg (voir *Mathesis*, t. I, p. 25).

Considérons l'ensemble de toutes les permutations, c'est-à-dire de toutes les solutions du problème des tours, en nombre P_n. Parmi celles-ci, le nombre des solutions ne contenant aucun élément à son rang, c'est-à-dire aucune tour sur la diagonale, est, par définition, égal à Q_n. Le nombre des solutions contenant une seule tour sur la diagonale est, comme on le voit en supprimant la ligne et la colonne contenant cette tour, nQ_{n-1}. En général, le nombre des solutions qui contiennent p tours sur la diagonale est

(¹) *Recherches sur une nouvelle espèce de carrés magiques* (*Mémoires de la Société des Sciences de Flessingue*, t. IX; 1779). — A propos de la relation (2), Euler ajoute : « Mais je dois avouer que je n'ai trouvé la propriété de déterminer chaque nombre par le seul précédent que par induction, et je ne vois pas trop bien comment on pourrait la déduire de la nature de la série. » Cette difficulté, signalée par Euler, a été résolue par M. Neuberg.

égal au produit de Q_{n-p} par le nombre des manières de placer p objets sur n cases, ou le nombre C_n^p des combinaisons de n objets pris p à p. Enfin le nombre des solutions contenant n tours sur la diagonale est 1; par conséquent, en posant conventionnellement $Q_0 = 1$, on a

$$P_n = Q_n + \frac{n}{1} Q_{n-1} + \frac{n(n-1)}{1.2} Q_{n-2} + \ldots + Q_0,$$

ou, symboliquement,

$$P^n \doteq (Q + 1)^n;$$

ainsi, les symboles P et $(Q+1)$ sont équivalents dans les formules algébriques; on a donc, avec une variable x, l'identité

$$(P + x)^n \doteq (Q + 1 + x)^n,$$

et en supposant $x = -1$, il vient

$$Q^n \doteq (P - 1)^n \quad \text{ou} \quad Q_n \doteq \Delta^n P_0.$$

Plus généralement, si l'on désigne par A_m^n le nombre des arrangements simples de m éléments pris n à n et par B_m^n le nombre des arrangements *discordants* avec un arrangement, c'est-à-dire des arrangements tels qu'aucun des éléments n'occupe la même place que dans l'arrangement donné, on a encore les formules suivantes, indiquées par M. NEUBERG :

$$A_m^n \doteq (1 + u)^n, \quad \text{avec} \quad u_p = B_{m-p}^{n-p};$$

$$B_m^n \doteq (1 - v)^n, \quad \text{»} \quad v_p = A_{m-p}^{n-p};$$

$$B_m^n \doteq n!\, \exp(-w), \quad \text{»} \quad w_p = C_{m-p}^{n-p}.$$

Après le développement des seconds membres, on doit remplacer les exposants de u, v, w par des indices, puis u_p, v_p, w_p par les valeurs indiquées, C désignant des combinaisons simples.

Exemple I. — Développer l'expression $(Q_n : P_n)$ en produit continu. On déduit des formules (1) et (2)

$$\frac{Q_n}{P_n} = \frac{Q_{n-1}}{P_{n-1}} \cdot \frac{Q_n}{Q_n - (-1)^n};$$

par suite, en remplaçant successivement n par 2, 3, ..., n, et en multipliant, membre à membre, les égalités obtenues, il vient

$$\frac{Q_n}{P_n} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{9}{8} \cdot \frac{44}{45} \cdots \frac{Q_n}{Q_n - (-1)^n}.$$

Ce calcul a été indiqué par M. HERMÈS (*Archives de* GRUNERT).

Exemple II. — Problème des ménages. — Des femmes, en nombre n, sont rangées autour d'une table, dans un ordre déterminé; on demande quel est le nombre des manières de placer leurs maris respectifs, de telle sorte qu'un homme soit placé entre deux femmes, sans se trouver à côté de la sienne?

Le problème revient évidemment à déterminer le nombre des permutations discordantes avec les deux permutations

$$\begin{cases} 1, & 2, & 3, & 4, & \ldots, & (n-1), & n, \\ 2, & 3, & 4, & 5, & \ldots, & n, & 1, \end{cases}$$

c'est-à-dire à déterminer le nombre des manières de placer n tours sur l'échiquier, de telle sorte que ces tours ne soient pas mutuellement en prise, et ne se trouvent pas situées sur les cases de la diagonale ascendante ↗, ni sur celles de la parallèle immédiatement au-dessus, ni sur le coin inférieur à droite.

Nous ne connaissons aucune solution simple de cette question, dont l'énoncé donne lieu à l'étude du nombre des permutations discordantes de deux permutations déjà discordantes et, plus généralement, du nombre des permutations discordantes de deux permutations quelconques.

124. Des permutations figurées, symétriques par rapport à une diagonale de l'échiquier. — Nous commencerons par déterminer le nombre D_n des permutations qui sont symétriques par rapport à la diagonale aa' (*fig.* 69). Deux cas peuvent se présenter, suivant que la tour placée dans la première colonne est au coin a de la diagonale, ou en b, case quelconque de cette colonne autre que a. Dans le premier cas, en supprimant la ligne et la colonne qui contiennent a, il reste un échiquier de $(n-1)$ cases de côté. Dans le second cas, à la tour b correspond nécessairement la tour b', symétrique par rapport à la diagonale. En supprimant les lignes et les colonnes qui contiennent b et b', il reste un ensemble de cases que l'on peut considérer comme celles d'un échiquier de $(n-2)$ cases de côté; mais b peut occuper $(n-1)$ places. On a donc la relation de récurrence

$$(1) \qquad D_n = D_{n-1} + (n-1) D_{n-2},$$

ou, en posant $D_n = u_n$, et en changeant n en $(n+1)$,

$$(2) \qquad \Delta u_n = n u_{n-1};$$

et, en général,

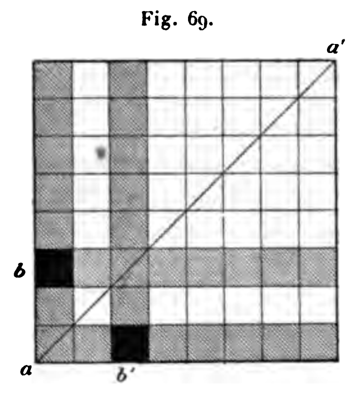
$$\frac{\Delta f(u)}{\Delta u} \triangleq \frac{d f(u)}{du}.$$

On trouve, par un calcul direct, les valeurs suivantes :

n	0,	1,	2,	3,	4,	5,	6,	7,	8,	...;
D_n	1,	1,	2,	4,	10,	26,	76,	232,	764,	....

La relation (1) ne permet pas d'obtenir facilement D_n en fonction de n; mais on y parvient de la manière suivante. Lorsque, dans une solution quelconque D_n, symétrique par rapport à la diagonale aa', on échange les colonnes contenant deux positions symétriques, telles que b et b', et qu'on fait la même opération pour tous les couples de positions symétriques, on replace toutes les tours sur la diagonale aa'. On voit donc que le nombre des solutions, dans lesquelles toutes les tours, à l'exception de *deux*, sont

Fig. 69.



situées sur la diagonale, est le nombre des combinaisons simples C_n^2; on voit ensuite que le nombre des solutions dans lesquelles toutes les tours, à l'exception de *quatre*, sont situées sur aa', est

$$\frac{1}{1.2} C_n^2 C_{n-2}^2;$$

puis on reconnaît que le nombre des solutions dans lesquelles

toutes les tours, à l'exception de *six*, sont situées sur la diagonale aa', est

$$\frac{1}{1.2.3} C_n^2 C_{n-2}^2 C_{n-4}^2,$$

et ainsi de suite. On a donc

$$D_n = 1 + \frac{1}{1} C_n^2 + \frac{1}{1.2} C_n^2 C_{n-2}^2 + \frac{1}{1.2.3} C_n^2 C_{n-2}^2 C_{n-4}^2 + \ldots,$$

c'est-à-dire

$$D_n = 1 + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)(n-3)}{2.4} + \frac{n(n-1)(n-2)(n-3)(n-4)(n-5)}{2.4.6} + \ldots,$$

ou encore, sous forme symbolique exponentielle,

$$D_n \triangleq \exp ax, \qquad \text{avec} \qquad a_p = \frac{A_n^{2p}}{2^p}.$$

125. Des permutations figurées qui sont symétriques par rapport aux deux diagonales de l'échiquier. — Nous observerons d'abord que toute solution symétrique par rapport aux deux diagonales est symétrique par rapport au centre; inversement, toute solution symétrique par rapport au centre et à l'une des diagonales l'est aussi par rapport à l'autre diagonale. Il suffit donc de considérer l'échiquier pair de $2n$ cases de côté, et, si l'on désigne par B le nombre des solutions, on a

$$B_{2n+1} = B_{2n}.$$

Il existe nécessairement une tour sur la première colonne; si on la suppose en un coin, a ou b (*fig.* 70), il en résulte la position d'une seconde au coin opposé a' ou b'. Mais si l'on suppose la tour de la première colonne à une case b (*fig.* 71) distincte d'un coin, il en résulte la position de trois autres tours en b', c, c'. Donc, en supprimant les lignes et les colonnes qui renferment des tours, il reste, dans le premier cas, un échiquier de $(2n-2)$ cases de

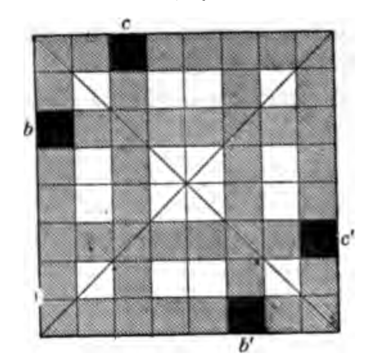
côté, et, dans le second, un ensemble de cases que l'on peut considérer comme un échiquier de $(2n - 4)$ cases de côté; mais,

Fig. 70.

dans le second cas, b peut occuper $(2n - 2)$ positions. On a donc la relation de récurrence

$$B_{2n} = 2B_{2n-2} + (2n - 2)B_{2n-4}$$

Fig. 71.



On trouve ainsi, pour les premières valeurs de n, les nombres suivants :

n	0,	1,	2,	3,	4,	5,	6,	7,	8,
B_n	1,	1,	2,	2,	6,	6,	20,	20,	76.

126. Des permutations figurées qui sont symétriques par rapport à une diagonale et qui n'ont aucune tour sur cette diagonale. — Nous désignerons par T_n le nombre des solutions pour

l'échiquier de n cases de côté; il est évident que le problème ne comporte aucune solution pour n impair; d'autre part, on voit facilement, par la considération de la *fig.* 69, que l'on a

$$T_{2n} = (2n-1)T_{2n-2};$$

par suite,

$$T_{2n} = 1.3.5\ldots(2n-1),$$

et

$$T_0 = 1, \qquad T_{2n+1} = 0.$$

Nous avons obtenu précédemment (n° **124**) le nombre D_n des permutations figurées qui sont symétriques par rapport à une diagonale. En appliquant le raisonnement de M. NEUBERG (n° **123**), au cas qui nous occupe, on trouve la formule symbolique

$$D^n \simeq (T+1)^n,$$

et, par suite (n° **121**),

$$T^n \simeq (D-1)^n.$$

127. Des permutations figurées qui sont symétriques par rapport au centre et qui n'ont aucune tour sur une diagonale. — Désignons par S_n le nombre cherché pour l'échiquier de n cases; on a d'abord, pour l'échiquier impair,

$$S_{2n+1} = 0.$$

Lorsque le côté $2n$ de l'échiquier est pair, on a trois cas à considérer :

1° La tour de la première colonne, à gauche, est au coin qui ne fait pas partie de la diagonale considérée ↗; alors, en supprimant les bords de l'échiquier, il reste un échiquier de $(2n-2)$ cases de côté; on a ainsi S_{2n-2} solutions.

2° La tour a de la première colonne n'étant pas dans un coin peut occuper $(2n-2)$ places; s'il existe, dans la ligne inférieure, une tour a' symétrique de a par rapport à la diagonale ↗, la suppression des lignes et des colonnes, contenant a, a' et les cases symétriques par rapport au centre, donne un ensemble de cases qui correspond à l'échiquier de $(2n-4)$ cases de côté; on a ainsi $(2n-2)S_{2n-4}$ solutions.

3° La tour est en a et la tour de la ligne inférieure n'est pas la symétrique de a par rapport à la diagonale; alors on échange les

deux colonnes, comme au n° **123**, ainsi que les colonnes symétriques par rapport au centre, et l'on supprime les bords de l'échiquier; il reste alors un échiquier de $(2n-2)$ cases de côté ; d'ailleurs a peut occuper $(2n-1)$ places. On a donc

$$S_{2n} = (2n-2)S_{2n-2} + (2n-2)S_{2n-4}.$$

Par la méthode de M. Neuberg, on trouvera, comme au n° **123**, l'identité symbolique

$$G^{2n} \simeq (S^2+1)^n, \quad \text{avec} \quad S_0 = 1, \quad G_0 = 1,$$

dans laquelle G_{2n} désigne le nombre des permutations figurées qui sont symétriques par rapport au centre de l'échiquier (n° **43**, *Ex. II*). Ainsi les symboles G^2 et (S^2+1) sont équivalents, et l'on a

$$S^{2n} \simeq (G^2-1)^n;$$

ou, en se reportant à la valeur de G_{2n},

$$S_{2n} = 2^n n! - \frac{n}{1} 2^{n-1}(n-1)! + \ldots + (-1)^n;$$

d'ailleurs, on a encore

$$G_{2n} = 2^n P_n, \quad \text{et} \quad S^{2n} \simeq (2P-1)^n.$$

128. Des permutations figurées qui sont symétriques par rapport aux deux diagonales de l'échiquier et qui ne contiennent aucune tour sur une ou deux diagonales. — Nous désignerons respectivement par U_n et par V_n les nombres des permutations qui ne contiennent aucune tour sur une diagonale, ou sur deux diagonales, dans l'échiquier de n cases de côtés. On a d'abord

$$U_{2n+1} = 0, \quad V_{2n+1} = 0, \quad V_2 = 0.$$

En se servant des méthodes employées précédemment, on obtient les formules de récurrence

$$U_{2n} = U_{2n-2} + (2n-2)U_{2n-4},$$
$$V_{2n} = (2n-2)V_{2n-4},$$

d'où l'on déduit

$$V_{4n} = 2.6.10\ldots(4n-2),$$
$$V_{4n+2} = 0.$$

Par l'analyse de M. Neuberg, on obtient les identités symboliques

$$B^{2n} \doteq (U^2 + 1)^n,$$
$$U^{2n} \doteq (B^2 - 1)^n,$$

et aussi

$$U^{2n} \doteq (V^2 + 1)^n,$$
$$V^{2n} \doteq (U^2 - 1)^n;$$

enfin, par comparaison avec les précédentes,

$$B^{2n} \doteq (V^2 + 2)^n.$$

En résumé, les permutations figurées étant désignées par les notations suivantes

P_n permutations figurées;
G_n symétriques au centre;
D_n symétriques à une diagonale;
B_n symétriques aux deux diagonales;
R_n symétriques par rotation d'un quart;

on forme, pour les premières valeurs de n, le Tableau :

n.	P_n.	G_n.	D_n.	B_n.	R_n.
0	1	1	1	1	1
1	1	1	1	1	1
2		2	2	2	0
3	6	2	4	2	0
4	24	8	10	6	2
5	120	8	26	6	2
6	720	48	76	20	0
7	5040	48	232	20	0
8	40320	384	764	76	12
9	3 62880	384	2620	76	12
10	36 28800	3840	9496	312	0
11	399 16800	3840	35696	312	0
12	4790 01600	46080	140152	1384	120

On peut facilement déterminer le nombre des solutions *primordiales*, en ne considérant pas comme distinctes les solutions que l'on peut déduire d'une première par rotation de l'échiquier pour un ou deux quarts de tour, ou par symétrie par rapport à l'une des médianes, ou à l'une des diagonales

de l'échiquier. Nous désignerons par la lettre grecque correspondante le nombre des solutions primordiales de chacun des groupes précédents.

En exceptant l'échiquier d'une case, toute solution ***bisymétrique*** soit par deux diagonales, soit par rotation d'un quart de tour, donne une autre solution; on a donc

$$B_n = 2\beta_n, \qquad R_n = 2\rho_n.$$

Toute solution *monosymétrique*, c'est-à-dire symétrique par rapport au centre ou par rapport à une seule diagonale, en produit trois autres; mais on doit tenir compte des solutions bisymétriques; on trouve ainsi

$$4\delta_n + 4\beta_n = 2D_n, \qquad 4\gamma_n = G_n - B_n - R_n;$$

ce qui détermine γ_n; on a ensuite

$$\beta_n = \tfrac{1}{2}B_n, \qquad \rho_n = \tfrac{1}{2}R_n, \qquad \delta_n = \tfrac{1}{2}D_n - \tfrac{1}{2}B_n.$$

Si α_n désigne le nombre des permutations primordiales qui ne présentent aucun caractère de symétrie, on a, puisque chacune d'elles en donne huit,

$$8\alpha_n + 4\delta_n + 4\gamma_n + 4\beta_n + 2\rho_n = P_n,$$

et ainsi

$$8\alpha_n = P_n - B_n - G_n - D_n.$$

Enfin, le nombre total σ_n des solutions primordiales est

$$\sigma_n = \alpha_n + \beta_n + \gamma_n + \delta_n + \rho_n.$$

On forme ainsi, pour les premières valeurs de n le Tableau suivant :

n.	α_n.	δ_n.	γ_n.	β_n.	ρ_n.	σ_n.
2	0	0	0	1	0	1
3	0	1	0	1	0	2
4	1	2	0	3	1	7
5	9	10	0	3	1	23
6	70	28	7	10	0	115
7	571	106	7	10	0	694
8	4820	344	74	38	6	5282
9	44676	1272	74	38	6	46066
10	4 50824	4592	882	156	0	4 56454
11	49 80274	17692	882	156	0	49 99004
12	598 34748	69384	11144	692	60	599 16028

Il nous reste à donner les valeurs numériques des solutions qui corres-

pondent aux premières valeurs de n pour les permutations restreintes, c'est-à-dire des permutations figurées qui n'ont aucune tour sur l'une des diagonales, ou sur les deux. Nous laissons au lecteur le soin de déterminer les nombres des solutions primordiales correspondantes.

Q_n permutations figurées simplement restreintes;
S_n symétriques au centre et restreintes par une diagonale;
T_n symétriques et restreintes par une diagonale;
U_n symétriques aux deux diagonales et restreintes par l'une d'elles;
V_n symétriques et restreintes pour les deux diagonales.

n.	Q_n.	S_n.	T_n.	U_n.	V_n.
0	1	1	1	1	1
1	0	0	0	0	0
2	1	1	1	1	0
3	2	0	0	0	0
4	9	5	3	3	2
5	44	0	0	0	0
6	265	29	15	7	0
7	1854	0	0	0	0
8	14833	233	105	25	12
9	1 33496	0	0	0	0
10	13 34961	2329	945	81	0
11	146 84570	0	0	0	0
12	1762 14841	27949	10395	331	120

Exemple I. — Déterminer le nombre des permutations figurées, symétriques par rapport à une diagonale de l'échiquier, et n'ayant aucune tour sur l'autre diagonale.

Exemple II. — On considère la suite

$$1, \quad 1, \quad 2, \quad 8, \quad 50, \quad 418, \quad \ldots,$$

dans laquelle $u_0 = u_1 = 1$, et

$$u_n = (2n-1)\, u_{n-1} - (n-1)\, u_{n-2};$$

démontrer que l'on a

$$2^n u_n = 1 + 1 \,.\, C_n^1 + 1 \,.\, 5 \,.\, C_n^2 + 1 \,.\, 5 \,.\, 9 \,.\, C_n^3 + \ldots .$$

(SYLVESTER).

CHAPITRE XIV.

SOMMATION DES PUISSANCES NUMÉRIQUES.

Nous exposerons dans ce Chapitre les principaux résultats sur le *Calcul des sommes,* que l'on appelle improprement *Calcul inverse des différences.* Ce calcul a pour but de déterminer la somme des valeurs numériques que prend un polynôme donné, lorsque l'on y remplace la variable par des nombres en progression arithmétique. En particulier, ce calcul donne la somme des puissances semblables des termes d'une progression arithmétique; plus particulièrement, il donne la somme des puissances semblables des nombres entiers.

La somme des carrés des premiers nombres entiers était connue d'Archimède, qui en a fait l'application à la détermination du volume de la pyramide et de l'aire du segment, dans la parabole et dans la spirale. On la trouve aussi dans les ouvrages des géomètres de l'Inde, et dans le *Liber Quadratorum* de Fibonacci. Les géomètres indiens ont encore donné la somme des cubes des n premiers nombres, au moyen d'une méthode fort originale que nous avons développée.

Le second procédé de sommation est celui de Fermat; il est général. Pour trouver la somme des valeurs numériques que prend un polynôme $f(x)$ lorsque l'on remplace la variable x par des entiers consécutifs, Fermat développe le polynôme $f(x)$ suivant une somme algébrique de factorielles dont les facteurs représentent des suites d'entiers consécutifs (n° 102), telles que

$$x,\quad x(x+1),\quad x(x+1)(x+2),\quad x(x+1)(x+2)(x+3),\quad \ldots;$$

ce procédé est le plus simple et le plus rapide, puisqu'il ne suppose que la théorie de la division algébrique. En appliquant à ce procédé la formule d'interpolation de Newton (n° 108), on obtient facilement le développement de $f(x)$ en somme de factorielles

consécutives, et ainsi, au moyen des formules du n° 37, on peut calculer rapidement

$$\Sigma f(x), \quad \Sigma\Sigma f(x), \quad \Sigma\Sigma\Sigma f(x),$$

pour des valeurs entières et consécutives de x, en progression arithmétique. Nous développons plus loin, au n° 137, la théorie générale de ce procédé.

Le troisième procédé a été exposé par PASCAL, dans son *Traité de la Sommation des puissances numériques*. Il consiste à calculer successivement, par récurrence, les sommes des puissances semblables des termes d'une progression arithmétique au moyen de toutes les sommes des puissances dont les exposants sont plus petits. C'est le procédé qui est habituellement employé dans tous les cours de Mathématiques; cependant, bien que nous l'ayons beaucoup perfectionné, il est notablement inférieur au procédé de FERMAT, et à celui de JACQUES BERNOULLI, dont nous allons dire quelques mots.

La somme des puissances semblables, d'exposant n, des x premiers termes d'une progression arithmétique est un polynôme de degré $(n+1)$, en x, ainsi qu'on le déduit immédiatement des deux procédés que nous venons d'indiquer; mais, si l'on met en évidence, dans le développement de ce polynôme, les coefficients de la puissance correspondante du binôme, on parvient à la connaissance d'une suite unique de nombres, que l'on appelle *nombres de Bernoulli*, qui se reproduisent pour tous les exposants. Ce fait remarquable permet alors d'établir des formules générales pour les sommations des puissances numériques.

Enfin nous rappellerons le procédé indiqué par ABEL, qui donne lieu à des formules intéressantes; mais c'est un procédé détourné que nous avons expliqué au n° 114 (*Ex. I*).

129. Sommation des carrés et des cubes. — Nous désignerons par $S_1, S_2, S_3, \ldots$ les sommes des n premiers nombres entiers, de leurs carrés, de leurs cubes, ... Pour obtenir la somme des carrés, on part de l'identité

$$(1) \qquad n^2 = (n-1)n + n;$$

si l'on y remplace successivement n par $1, 2, 3, \ldots, n$, et si l'on

fait la somme des égalités obtenues, il vient par la formule de sommation des factorielles (n° 37)

$$S_2 = \tfrac{1}{3}(n-1)n(n+1) + \tfrac{1}{2}n(n+1);$$

en simplifiant, on trouve la formule déjà obtenue (n° 39)

$$S_2 = \tfrac{1}{6}n(n+1)(2n+1).$$

Pour avoir la somme des cubes, multiplions le premier membre et le dernier terme de l'identité (1) par n, et le premier terme du second membre par $(n+1)-1$, afin d'introduire des factorielles; il en résulte l'identité

$$(2)\qquad n^3 = (n-1)n(n+1) + n;$$

si l'on y remplace successivement n par 1, 2, 3, ..., n, et si l'on fait la somme des égalités obtenues, il vient

$$S_3 = \tfrac{1}{4}(n-1)n(n+1)(n+2) + \tfrac{1}{2}n(n+1);$$

en remplaçant $n(n+1)$ par $2S_1$, et $(n-1)(n+2)$ par $(2S_1-2)$,

$$S_3 = (S_1)^2.$$

Exemple I. — On partage la suite des nombres impairs en groupes contenant respectivement 1, 2, 3, ..., p termes; trouver la somme des p termes du groupe de rang p.

Le groupe de rang p est une progression arithmétique de raison 2, contenant p termes et dont le premier a pour expression

$$1 + \frac{(p-1)p}{2}.2 \quad \text{ou} \quad p^2 - p + 1;$$

la somme des termes de ce groupe est donc égale à p^3. Cette propriété a été indiquée par Nicomaque, de Gérase (100 ans environ après J.-C.). Par suite, la somme des n premiers cubes vaut la somme des S_1 premiers nombres impairs, nombre égal à celui des termes des p premiers groupes; ainsi, encore, on démontre que $S_3 = (S_1)^2$.

Exemple II. — On partage la progression arithmétique commençant par 1 et de raison $(q-2)$ en groupes contenant respectivement 1, 2, 3, 4, ..., p termes; trouver la somme des termes du groupe de rang p et la somme des termes des n premiers groupes.

On trouve, pour le groupe de rang p,

$$p^3 + (q-4)\frac{(p-1)p(p+1)}{2};$$

par conséquent, si l'on fait la somme de tous les termes renfermés dans

les n premiers groupes (leur nombre est égal au polygonal de q côtés dont le rang est le $n^{\text{ième}}$ triangulaire S_1), on obtient le carré de ce triangulaire S_1. augmenté du triangulo-triangulaire de rang $(n-1)$ multiplié par $3(q-4)$. En d'autres termes,

$$\left[\frac{n(n+1)}{2}\right]^2 + 3(q-4)\frac{(n-1)n(n+1)(n+2)}{1.2.3.4}.$$

Le théorème précédent est une interprétation d'un passage obscur de Fermat, qui se trouve à la suite de la proposition 27, livre II, de l'Appendice de Bachet aux nombres polygonaux (voir notre Mémoire : *Sur un théorème de l'Arithmétique indienne*, publié dans le *Bullettino di Bibliografia,* t. IX; Rome, 1876).

Exemple III. — On partage la progression arithmétique commençant par 1 et de raison 4, qui produit les nombres hexagonaux, en groupes contenant respectivement 1, 3, 5, 7, ... termes; trouver la somme des termes du groupe de rang p.

Ce groupe est une progression arithmétique de raison 4, contenant $2p-1)$ termes, dont le premier est

$$1 + 4(p-1)^2;$$

par conséquent, la somme des termes de ce groupe est

$$[1 + 4(p-1)^2 + 2(2p-2)](2p-1), \quad \text{ou} \quad (2p-1)^3.$$

On en déduit que la somme des n premiers cubes impairs est égale au nombre hexagonal de rang n^2, c'est-à-dire à $n^2(2n^2-1)$.

Exemple IV. — On partage la suite des nombres entiers en groupes contenant respectivement 1, 2, 3, 4, ... termes; démontrer que la somme des termes renfermés dans les n premiers groupes de rang impair est égale à n^4.

Exemple V. — Pour quelle valeur de x la somme des carrés des $(n+1)$ entiers consécutifs, dont le dernier est x^2, vaut-elle la somme des carrés des n entiers suivants; quelle est cette somme?

On doit poser

$$(x-n)^2 + (x-n+1)^2 + \ldots + (x-1)^2 + x^2$$
$$= (x+1)^2 + (x+2)^2 + \ldots + (x+n)^2,$$

c'est-à-dire

$$x^2 = \sum_{p=1}^{p=n} [(x+p)^2 - (x-p)^2] = \sum_{p=1}^{p=n} 4px,$$

d'où l'on tire

$$x = 2n(n+1);$$

la somme de ces carrés est

$$(12n^2 + 12n + 1)S_2.$$

130. Sommation des bicarrés. — Reprenons l'identité

$$n^3 = (n-1)n(n+1) + n;$$

multiplions par n le premier membre et le dernier terme du second membre, et par $(n+2) - 2$ le premier terme du second membre, afin d'obtenir des factorielles ; il vient

$$n^4 = (n-1)n(n+1)(n+2) - 2(n-1)n(n+1) + n^2.$$

Remplaçons successivement n par 1, 2, 3, ..., n, et ajoutons les égalités obtenues ; nous avons

$$S_4 = \tfrac{1}{5}(n-1)n(n+1)(n+2)(n+3) - \tfrac{1}{2}(n-1)n(n+1)(n+2) + S_2;$$

remplaçons $n(n+1)$ par $2S_1$, et $(n-1)(n+2)$ par $(2S_1 - 2)$, il vient tout de suite

$$5S_4 = (4n+2)(S_1)^2 - S_2,$$

et encore, en remplaçant $(4n+2)S_1$ par $6S_2$,

$$5S_4 = S_2(6S_1 - 1).$$

La première des deux formules précédentes a été donnée par Fermat dans sa lettre à Roberval du 4 novembre 1636 : « Si vous multipliez le quadruple du plus grand nombre augmenté de 2 par le carré du triangle de ce nombre, et si du produit vous retranchez la somme de leurs carrés, vous obtiendrez la somme quintuple de leurs quatrièmes puissances. Il semble que Bachet, dans son Traité des *Multangulis*, n'a pas voulu tâter ces questions, après avoir fait celle des carrés et des cubes. Je serais bien aise que vous vous exerciez pour trouver la méthode générale, pour voir si nous nous rencontrerons. »

Avant Fermat, la somme des n premiers bicarrés a été donnée par le médecin Djamchid ben Mas'oud, qui prit part à la rédaction des Tables astronomiques d'Ouloug-Beg. On lit dans un manuscrit conservé au *British Museum*, daté de 1589 (997 de l'hégire), un passage qui a été traduit ainsi : « Si nous désirons connaître la somme des bicarrés, nous retranchons 1 de la somme des premiers nombres et nous prenons constamment le cinquième du reste ; nous l'ajoutons à la somme desdits nombres et nous multiplions ce qui en provient par la somme des carrés des mêmes nombres. » On a donc

$$S_4 = \left(\frac{S_1 - 1}{5} + S_1\right) S_2,$$

formule équivalente à celle du texte, et préférable dans l'application à celle de Fermat, puisqu'elle donne le quotient de S_4 par S_2.

Cependant, c'est à FERMAT que l'on doit le principe de la méthode générale pour trouver les sommes des puissances semblables des nombres entiers. Il dit encore, dans la lettre que nous venons de rappeler : « *Il faut, étant donné un nombre,* in progressione naturali, *trouver la somme non seulement de tous les carrés et cubes, ce que les auteurs qui ont écrit ont déjà fait, mais encore la somme des carré-carrés, des carré-cubes, etc., ce que personne que je sache n'a encore trouvé, et pourtant cette connaissance est belle et de grand usage, et n'est pas des plus aisées; j'en suis venu à bout avec beaucoup de peine.* »

Exemple I. — La somme alternée des carrés des $2n$ premiers nombres impairs est égale à $-8n^2$.

Exemple II. — On partage la suite des nombres impairs en groupes tels que le $n^{\text{ième}}$ groupe ait $(1+2+3+\ldots+n)$ termes; la somme des termes de ce groupe est égale au produit

$$(1+2+3+\ldots+n)(1^2+2^2+3^2+\ldots+n^2).$$

Exemple III. — On partage la suite des nombres impairs en groupes tels que le $n^{\text{ième}}$ groupe ait an termes; la somme des termes de ce groupe est a^2n^3.

Exemple IV. — La somme des n^2 nombres entiers, qui suivent les n premiers, est double de la somme des n premiers cubes.

Exemple V. — On partage la suite naturelle des nombres en groupes tels que le $n^{\text{ième}}$ ait p^n termes; la somme des termes de ce groupe est

$$\frac{p^n(p^n-1)(p+1)}{2(p-1)}.$$

Exemple VI. — Si l'on fait de même, pour la suite des nombres impairs, le groupe de rang n a pour somme

$$\frac{p^{n+1}(p^n+p^{n-1}-2)}{p-1}.$$

Exemple VII. — On partage la suite des nombres impairs en groupes consécutifs comprenant chacun un même nombre p de termes. Quels sont les groupes dont la somme est un carré?

Ceux dont le rang est la somme de deux carrés consécutifs.

Exemple VIII. — Si l'on partage la suite des cubes en groupes consécutifs tels que le $n^{\text{ième}}$ renferme n termes, la somme des termes du $n^{\text{ième}}$ groupe est

$$\tfrac{1}{8}n^3(n^2+1)(n^2+3).$$

Exemple II. [illegible] de rang impair augmentée [illegible]

Exemple X. [illegible] impairs en groupes [illegible] $n^{ième}$ renferme n termes, la somme des termes de ce groupe est [illegible]

Exemple XI. La différence entre le cube de la somme et la somme des cubes des n premiers nombres impairs est un carré.

Les énoncés des neuf exercices qui précèdent sont dus à M. DE ROCQUIGNY (*Mathesis*, t. V).

Exemple XII. On considère les deux suites des n premiers nombres entiers

$$\begin{matrix} 1, & 2, & 3, & \ldots & (n-2), & (n-1), & n, \\ n, & (n-1), & (n-2), & \ldots & 3, & 2, & 1; \end{matrix}$$

on multiplie chaque terme de la première par le terme placé au-dessous. La somme des produits obtenus est égale au $n^{ième}$ nombre pyramidal.

Fig. 29.

```
o         o          o          o          o
   o  o      o  o       o  o       o  o
           o  o  o     o  o  o    o  o  o
                   o  o  o  o   o  o  o  o
                                o  o  o  o  o
```

[illegible] de la pile triangulaire.

[illegible] (fig. 29), en faisant la [illegible]

[illegible] deux suites

[illegible]

[illegible]

Exemple XIV. — Si l'on fait la somme des boulets contenus dans les n premières piles triangulaires, en groupant les tranches de même rang, à partir du haut, on trouve (n° 38)

$$1.n(n+1)+2(n-1)n+\ldots+(n-1).2.3+n.1.2=\frac{n(n+1)(n+2)(n+3)}{12}.$$

Exemple XV. — En opérant de même sur les piles à base carrée, on a (n° 38)

$$1.n^2+2.(n-1)^2+3.(n-2)^2+\ldots+(n-1).2^2+n.1^2=\frac{n(n+1)^2(n+2)}{12}.$$

Exemple XVI. — On considère les deux suites

$$\begin{array}{ccccc} 1^2, & 2^2, & \ldots, & (n-1)^2, & n^2, \\ n^2, & (n-1)^2, & \ldots, & 2^2, & 1^2; \end{array}$$

on multiplie chaque terme de la première par le terme placé au-dessous; la somme des produits obtenus est

$$\tfrac{1}{30}(n+1)[(n+1)^4-1].$$

Exemple XVII. — Même question, en remplaçant les n premiers nombres entiers par les n premiers nombres impairs.

On trouve

$$\tfrac{1}{15}n(8n^4+7).$$

Exemple XVIII. — Dans un jeu de dominos jusqu'au double n, on remplace le domino (a, b) par a^p+b^p; trouver la somme des points obtenus après cette transformation?

Considérons les arrangements complets des nombres 0, 1, 2, ..., n, pris deux à deux, rangés comme dans la table de Pythagore; remplaçons chaque nombre a par a^p; en faisant la somme, par lignes ou par colonnes, on trouve $(2n+2)$ fois la somme S_p des puissances d'exposant p des n premiers nombres; ajoutons deux fois la somme S_p pour les doubles. Les dominos ayant été comptés deux fois, la somme cherchée est égale à $(n+2)S_p$.

Mêmes questions, en remplaçant le domino (a, b) par $(a+b)^p$, ou encore par $(ab)^p$.

Exemple XIX. — La somme des n premiers triangulaires de rang pair a pour expression

$$\tfrac{1}{6}n(n+1)(4n+5).$$

131. Méthode indienne. — Considérons la Table de multiplication continuée jusqu'au produit de n par n; la somme des

pour le développement de S_{p-1}. Mais on doit constater ce *fait remarquable*, que si l'on passe de la somme S_{p-1} à la somme S_p, pour l'exposant suivant, il suffit d'ajouter, aux équations (2), une nouvelle équation

$$(B+1)^{p+1} - B^{p+1} \triangleq 0,$$

tout en conservant les précédentes; on n'a qu'un seul nouveau coefficient B_p à calculer. On a donc le théorème suivant (¹) :

Si l'on désigne par B_0, B_1, B_2, ... *une suite de nombres déterminés successivement par des équations de la forme*

$$(3) \qquad (B+1)^n - B^n \triangleq 0,$$

avec les conditions initiales $B_0 = 1$, $B_1 = -\frac{1}{2}$, *et pour* $n > 1$, *on a l'identité*

$$(4) \qquad p\,S_{p-1} \triangleq (x+B)^p - B^p.$$

Les coefficients B ont été appelés par Euler les *Nombres de Bernoulli;* pour la somme des puissances des x premiers nombres, on remplace $B_1 = -\frac{1}{2}$ par $B'_1 = +\frac{1}{2}$. D'ailleurs, puisque S_{2p-1} est divisible par S_3 et, par conséquent, par x^2, *les nombres de Bernoulli d'indice impair sont nuls, à l'exception de* $B_1 = \mp\frac{1}{2}$.

De la formule (4), on tire

$$\frac{dS_p}{dx} \triangleq p\,S_{p-1} + B_p;$$

cette formule permet de déterminer S_p par voie d'intégration, en calculant chaque fois la constante B_p par l'une ou l'autre des conditions $S_p = 1$ pour $x = 2$, et $S_p = 0$ pour $x = 1$.

(¹) Ce théorème a été donné sous une forme différente par Jacques Bernoulli (*Ars conjectandi*, 1713); la formule (4) a été indiquée par Moivre dans ses *Miscellanea analytica*, mais aussi sous une forme différente. Nous devons faire observer que, pour la simplification des formules de cette théorie, nous avons dû modifier les diverses notations, employées jusqu'ici, des nombres de Bernoulli.

On trouve ainsi, pour les premières valeurs de p,

$$
\begin{aligned}
S_1 &= \tfrac{1}{2}x^2 \mp \tfrac{1}{2}x,\\
S_2 &= \tfrac{1}{3}x^3 \mp \tfrac{1}{2}x^2 + \tfrac{1}{6}x,\\
S_3 &= \tfrac{1}{4}x^4 \mp \tfrac{1}{2}x^3 + \tfrac{1}{4}x^2,\\
S_4 &= \tfrac{1}{5}x^5 \mp \tfrac{1}{2}x^4 + \tfrac{1}{3}x^3 - \tfrac{1}{30}x,\\
S_5 &= \tfrac{1}{6}x^6 \mp \tfrac{1}{2}x^5 + \tfrac{5}{12}x^4 - \tfrac{1}{12}x^2,\\
S_6 &= \tfrac{1}{7}x^7 \mp \tfrac{1}{2}x^6 + \tfrac{1}{2}x^5 - \tfrac{1}{6}x^3 + \tfrac{1}{42}x,\\
S_7 &= \tfrac{1}{8}x^8 \mp \tfrac{1}{2}x^7 + \tfrac{7}{12}x^6 - \tfrac{7}{24}x^4 + \tfrac{1}{12}x^2,\\
S_8 &= \tfrac{1}{9}x^9 \mp \tfrac{1}{2}x^8 + \tfrac{2}{3}x^7 - \tfrac{7}{15}x^5 + \tfrac{2}{9}x^3 - \tfrac{1}{30}x,\\
S_9 &= \tfrac{1}{10}x^{10} \mp \tfrac{1}{2}x^9 + \tfrac{3}{4}x^8 - \tfrac{7}{10}x^6 + \tfrac{1}{2}x^4 - \tfrac{3}{20}x^2,\\
S_{10} &= \tfrac{1}{11}x^{11} \mp \tfrac{1}{2}x^{10} + \tfrac{5}{6}x^9 - x^7 + x^5 - \tfrac{1}{2}x^3 + \tfrac{5}{66}x,\\
S_{11} &= \tfrac{1}{12}x^{12} \mp \tfrac{1}{2}x^{11} + \tfrac{11}{12}x^{10} - \tfrac{11}{8}x^8 + \tfrac{11}{6}x^6 - \tfrac{11}{8}x^4 + \tfrac{5}{12}x^2.
\end{aligned}
$$

Le signe — se rapporte à la somme des puissances des $(x-1)$ premiers entiers et le signe + à celle des puissances des x premiers.

Mais, pour de plus grandes valeurs de p, il est préférable de développer la formule (4) en mettant en évidence les coefficients du binôme et les nombres bernoulliens, qui ont été calculés par M. ADAMS jusqu'à B_{124}. Quant aux nombres B, leur calcul le plus rapide se fait au moyen des formules données dans le numéro suivant, ou encore par l'emploi du beau théorème de CLAUSEN et de STAUDT, qui sera énoncé et démontré au Livre III.

135. Nombres de Bernoulli. — On a, pour les premiers nombres, les valeurs

$$
\begin{array}{lll}
B_2 = +\dfrac{1}{6}, & B_4 = -\dfrac{1}{30}, & B_6 = +\dfrac{1}{42},\\[2ex]
B_8 = -\dfrac{1}{30}, & B_{10} = +\dfrac{5}{66}, & B_{12} = -\dfrac{691}{2730},\\[2ex]
B_{14} = +\dfrac{7}{6}, & B_{16} = -\dfrac{3617}{510}, & B_{18} = +\dfrac{43867}{798},\\[2ex]
B_{20} = -\dfrac{174611}{330}, & B_{22} = +\dfrac{854513}{138}, & B_{24} = -\dfrac{236364091}{2730},\\[2ex]
B_{26} = +\dfrac{8553103}{6}, & B_{28} = -\dfrac{23749461029}{870}, & B_{30} = +\dfrac{8615841276005}{14322}.
\end{array}
$$

Ces nombres jouent un très grand rôle dans l'Analyse mathématique; nous allons donner quelques autres formules importantes. Désignons par $f(x)$ un polynôme entier quelconque

$$f(x) = a_0x^p + a_1x^{p-1} + \ldots + a_px^0,$$

et reprenons l'identité symbolique

$$(x+1+B)^n - (x+B)^n \triangleq nx^{n-1};$$

si nous y remplaçons successivement n par p, $(p-1)$, ..., 3, 2, 1, et si nous ajoutons les égalités obtenues, après avoir multiplié respectivement par a_0, a_1, ..., a_{p-1}, il vient

$$(1) \qquad f(x+B+1) - f(x+B) \triangleq f'(x).$$

C'est l'*identité symbolique fondamentale* pour le calcul des nombres bernoulliens. Si l'on suppose successivement que $f(x)$ représente

$$(2x-1)^p, \quad x(x+1)\ldots(x+p), \quad (x-1)x\ldots(x+p-1),$$

on trouve, en faisant ensuite $x = 0$, les formules de récurrence

$$(2B+1)^p - (2B-1)^p \triangleq 2p(-1)^{p-1},$$
$$(p+1)(B-1)(B+2)\ldots(B+p) \triangleq p!,$$
$$(p+1)B(B+1)\ldots(B+p-1) \quad \triangleq -(p-1)!.$$

Si l'on suppose encore

$$f(x) = (x-1)^p x^q,$$

pour p et $(q-1)$ entiers et positifs, l'identité fondamentale donne la relation

$$B^p(B+1)^q - B^q(B-1)^p \triangleq 0.$$

Cette formule présente, pour le calcul, l'avantage de ne pas contenir tous les coefficients B, mais seulement ceux dont l'indice est compris entre B_{p+q} et B_q, en supposant $q < p$. Elle a été indiquée par Stern (*Journal de Crelle*, t. 84, p. 216); la démonstration précédente, qui la rattache à notre identité fondamentale, a été donnée par M. Radicke (*Journal de Crelle*, t. 89, p. 259).

Exemple I. — Démontrer la formule

$$(B+2)(B+3)\ldots(B+p) \doteq (p-1)!\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{p}\right).$$

Exemple II. — Démontrer la formule

$$B^p(B+1)^q(B+2)^r(B+3)^s \doteq B^s(B-1)^r(B-2)^q(B-3)^p,$$

dans laquelle p, $q-1$, $r-1$, $s-1$ sont des entiers positifs.

On pose dans l'identité fondamentale

$$f(x) = x^p(x+1)^q(x+2)^r(x+3)^s;$$

on remplace ensuite x par -1, -2, -3, et l'on fait la e des égalités obtenues.

On peut trouver des formules analogues pour les sommes S.

Exemple III. — L'identité fondamentale (1) peut être généralisée. En effet, on peut, avec les notations des différences et des différentielles, l'écrire sous la forme

$$\Delta f(x+B) \doteq \frac{df}{dx},$$

en supposant $\Delta x = 1$; de même, par l'introduction d'une autre variable y, et pour des accroissements de x et de y égaux à 1,

$$\Delta^2_{x,y} f(x+B,\, y+B') \doteq \frac{\partial^2 f(x,y)}{\partial x\, \partial y},$$

et ceci s'applique à un nombre quelconque de variables. Il ne faut pas réduire les B avec les B′, les B″, ...; mais, lorsque le développement symbolique du premier membre sera effectué, on remplacera les exposants de B, B′, B″, ..., par des indices. On obtiendra ainsi des relations contenant les produits deux à deux, trois à trois, ... des nombres de BERNOULLI (*Comptes rendus des séances de l'Académie des Sciences;* Paris, 1876).

Nous allons encore démontrer la formule générale

$$(2) \qquad f(Bx+S) + f(Bx) \doteq x f(B),$$

dans laquelle on remplace, après développement, les exposants de B et de S par des indices.

En effet, considérons le polynôme en y

$$y^p + (y+1)^p + (y+2)^p + \ldots + (y+x-1)^p;$$

si l'on fait la somme, on obtient une première expression

$$y^p = \frac{(y+x+B)^{p+1} - (y+B)^{p+1}}{p+1}.$$

Ce résultat subsiste lorsque l'on remplace y par une quantité symbolique, et, par exemple, par $B'x$, en désignant par B' les nombres bernoulliens; mais, si l'on se rappelle que $(B+1)^n - B^n$ s'annule pour $n > 1$ et devient l'unité pour $n = 1$, l'expression précédente, où l'on remplace y par Bx, devient xB_p; on a donc

$$(3) \qquad (Bx)^p + (Bx+1)^p + \ldots + (Bx+x-1)^p \doteq xB_p,$$

et, par l'emploi du symbole S,

$$(4) \qquad (Bx+S)^p - (Bx)^p \doteq xB^p;$$

d'où l'on déduit ensuite la formule (2).

En particulier, pour $x = 2$, la formule (3) devient

$$(5) \qquad (2B+1)^p + (2B)^p \doteq 2B^p;$$

par conséquent, les nombres de Bernoulli vérifient la relation

$$(6) \qquad f(2B+1) + f(2B) \doteq 2f(B).$$

136. Formules générales de sommation. — Soient $f(x)$ un polynôme quelconque et $F(x)$ le polynôme intégral, l'identité fondamentale du numéro précédent peut être écrite ainsi

$$f(x) \doteq F(x+B+1) - F(x+B).$$

Si l'on remplace successivement x par $0, 1, 2, \ldots, (x-1)$, et si l'on fait la somme des égalités obtenues, il vient

$$f(0) + f(1) + f(2) + \ldots + f(x-1) \doteq F(x+B) - F(B).$$

En se servant des notations du Calcul intégral, on a la formule symbolique suivante, dont l'application est très facile,

$$(1) \qquad \sum_{x=0}^{x=n-1} f(x) \doteq \int_B^{n+B} f(x)\,dx.$$

Pour obtenir les sommes de deux en deux, nous reprendrons la formule

$$(x+B+1)^p - (x+B)^p \doteq px^{p-1}.$$

Si l'on remplace x par $\frac{1}{2}x$, il vient, en multipliant par 2^p,

$$(x+2B+2)^p-(x+2B)^p=2px^{p-1}$$

et, par suite,

$$F(x+2B+2)-F(x+2B)=2f(x).$$

Remplaçons successivement x par $1, 3, 5, \ldots, (2x-1)$; en ajoutant les égalités obtenues, il vient

$$f(1)+f(3)+f(5)+\ldots+f(2x-1)=\tfrac{1}{2}F(2x+2B+1)-\tfrac{1}{2}F(2B+1).$$

On a de même

$$f(0)+f(2)+f(4)+\ldots+f(2x-2)=\tfrac{1}{2}F(2x+2B)-\tfrac{1}{2}F(2B).$$

Par le même procédé, on trouvera les sommes de 3 en 3, ..., de r en r, ..., et l'on généralisera la formule (1).

137. Extension de la méthode de Fermat. — Soit $f(x)$ un polynôme en x de degré n, la formule d'interpolation de NEWTON conduit à l'identité

$$f(x)=f(0)+\frac{x-x_0}{h}\frac{\Delta f(0)}{1!}+\frac{x-x_0}{h}\left(\frac{x-x_0}{h}-1\right)\frac{\Delta^2 f(0)}{2!}+\ldots.$$

On développe ainsi $f(x)$ en une somme algébrique de factorielles; si l'on remplace x par des nombres en progression arithmétique de raison h, on trouve par l'application de la formule qui donne la sommation des factorielles (n° 37) la somme des valeurs que prend le polynôme $f(x)$ pour des valeurs de x en progression arithmétique.

Mais le résultat est lui-même un polynôme de degré $(n+1)$ développé en une somme algébrique de factorielles, et l'on peut lui appliquer la formule fondamentale indiquée par FERMAT; par conséquent, on pourra trouver, d'une manière simple et générale, la valeur de l'expression

$$\Sigma\Sigma\Sigma\ldots f(x)$$

pour des valeurs de x égales aux termes successifs d'une progression arithmétique.

Soit, en particulier,

$$f(x) = x^n, \qquad \Delta x = h = 1 \qquad \text{et} \qquad x_0 = 0,$$

on a

$$(1) \qquad x^n = x\,\Delta 0^n + \frac{x(x-1)}{1.2}\Delta^2 0^n + \frac{x(x-1)(x-2)}{1.2.3}\Delta^3 0^n + \ldots;$$

par suite, en désignant par S_n la somme des puissances $n^{\text{ièmes}}$ des $(x-1)$ premiers nombres entiers, on a

$$(2) \qquad \begin{cases} S_n = \dfrac{x(x-1)}{1.2}\Delta 0^n + \dfrac{x(x-1)(x-2)}{1.2.3}\Delta^2 0^n \\ \qquad + \dfrac{x(x-1)(x-2)(x-3)}{1.2.3.4}\Delta^3 0^n + \ldots. \end{cases}$$

Cette formule montre que S_n est un polynôme en x de degré $(n+1)$, divisible par $x(x-1)$, et dont le premier coefficient est $\frac{1}{n+1}$ (n° 133). La formule (2) n'est qu'une transformation d'une propriété d'un tableau de sommes (n° 75).

D'ailleurs, si l'on prend le coefficient de x dans le développement de la formule qui précède, on exprime les nombres de Bernoulli en fonction des différences de x^n pour $x = 0$; on a ainsi

$$(3) \qquad B_n = -\frac{\Delta 0^n}{2} + \frac{\Delta^2 0^n}{3} - \frac{\Delta^3 0^n}{4} + \ldots + (-1)^n \frac{\Delta^n 0^n}{n+1}.$$

Exemple I. — Soit à calculer S_3. On forme le Tableau

Δ^3	Δ^2	Δ	x^3	x
6	6	1	0	0
	12	7	1	1
		19	8	2
			27	3

et l'on a

$$S_3 = \frac{x(x-1)}{1.2}1 + \frac{x(x-1)(x-2)}{1.2.3}6 + \frac{x(x-1)(x-2)(x-3)}{1.2.3.4}6.$$

En simplifiant, on retrouve le résultat connu. Cette méthode paraît moins simple dès l'abord; mais elle est la plus commode, lorsque l'on veut obtenir les sommes successives.

Exemple II. — Trouver la somme

$$1(x-1)^3+2(x-2)^3+3(x-3)^3+\ldots+(x-2)2^3+(x-1)1^3.$$

138. Sommations successives des puissances. — Posons

$$S_{1,n}(x)=1^n+2^n+3^n+\ldots+x^n,$$

en désignant par n un entier nul ou positif; posons ensuite

$$S_{2,n}(x)=S_{1,n}(1)+S_{1,n}(2)+\ldots+S_{1,n}(x),$$

et, en général,

$$S_{p+1,n}(x)=S_{p,n}(1)+S_{p,n}(2)+\ldots+S_{p,n}(x);$$

les sommes $S_{1,n}$, $S_{2,n}$, ... correspondent aux sommations successives.

Nous supposerons $S_{0,0}=1$; on a d'ailleurs, par la sommation des factorielles (n° 37),

$$S_{p,0}=\frac{x(x+1)\ldots(x+p-1)}{1.2.3\ldots p}.$$

Nous allons calculer $S_{2,n}$; pour cela, considérons le Tableau

$$\begin{array}{l}1^n\\1^n+2^n\\1^n+2^n+3^n\\1^n+2^n+3^n+4^n\\\ldots\ldots\ldots\ldots\ldots\ldots\\\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\1^n+2^n+3^n+4^n+\ldots+x^n;\end{array}$$

en faisant la somme par colonnes, on obtient pour la somme des termes de la colonne de rang p

$$(x-p+1)p^n \quad \text{ou} \quad (x+1)p^n-p^{n+1};$$

donc, en faisant le total de toutes les colonnes, on a

$$(1)\qquad S_{2,n}=(x+1)S_{1,n}-S_{1,n+1}.$$

Sous forme symbolique, la formule précédente peut s'écrire

$$S_{2,n} \triangleq S_1^n(x+1-S_1).$$

On trouve, par induction, la formule générale

$$(2)\qquad S_{p+1,n}(x) = \frac{1}{p!}\,S_1^n\,[x+1-S_1]\,[x+2-S_1]\ldots[x+p-S_1],$$

que l'on vérifie *a posteriori* en observant que, si l'on remplace x par $(x+1)$, le premier membre augmente de

$$S_{p,n}(x+1),$$

et le second devient

$$\frac{1}{p!}\,S_1^n\,[x+2-S_1]\,[x+3-S_1]\ldots[x+p+1-S_1],$$

et, par conséquent, augmente de

$$\frac{1}{(p-1)!}\,S_1^n\,[x+2-S_1]\,[x+3-S_1]\ldots[x+p-S_1];$$

c'est précisément ce que devient le second membre de la formule (2), quand on y remplace p par $(p-1)$ et x par $(x+1)$.

Exemple I. — Calculer les valeurs de $S_{2,n}$ pour $n = 1, 2, 3, 4$.
On trouve successivement

$$\begin{aligned}
S_{2,1} &= \tfrac{1}{6}\,x(x+1)(x+2),\\
S_{2,2} &= \tfrac{1}{12}\,x(x+1)^2(x+2),\\
S_{2,3} &= \tfrac{1}{60}\,x(x+1)(x+2)(x^2+6x+3),\\
S_{2,4} &= \tfrac{1}{60}\,x(x+1)^2(x+2)(2x^2+4x-1).
\end{aligned}$$

Pour plus de détails, *voir* nos articles du *Messenger of Mathematics*, intitulés : *On the Development of* $\left(\frac{z}{1-e^{-z}}\right)^x$ *in a Series* et *On the successive Summations* (Cambridge, 1877).

139. Extension de la méthode indienne. — Considérons la suite de x quantités

$$u_1,\quad u_2,\quad u_3,\quad \ldots,\quad u_p,\quad \ldots,\quad u_x;$$

formons une Table de multiplication en écrivant successivement les uns au-dessous des autres les produits des termes de cette suite par ceux de la suite

$$v_1,\quad v_2,\quad v_3,\quad \ldots,\quad v_p,\quad \ldots,\quad v_x;$$

la somme des termes de la Table sera égale au produit des sommes U_x et V_x des termes des deux suites. D'autre part, en ne prenant que les p premiers termes du Tableau qui se trouvent dans la ligne de rang p et les $(p-1)$ premiers dans la colonne de rang p, on a pour leur somme

$$u_p V_p + v_p U_p - u_p v_p;$$

par suite, en faisant la somme $\sum$ de ces expressions de $p=1$ à $p=x$, on a

$$(1) \qquad U_x V_x - \sum_{p=1}^{p=x} (u_p V_p + v_p U_p) + \sum_{p=1}^{p=x} u_p v_p = 0.$$

Considérons, de même, une troisième suite de quantités

$$w_1, \quad w_2, \quad w_3, \quad \ldots, \quad w_p, \quad \ldots, \quad w_x,$$

et plaçons les unes au-dessous des autres les Tables obtenues en multipliant tous les termes de la première Table successivement par tous les termes de la troisième suite; nous formons ainsi une Table de multiplication à trois entrées, et le compartiment de coordonnées p, q, r contiendra le produit $u_p v_q w_r$. Cela posé, considérons successivement les cubes ayant à partir de l'origine 1, 2, 3, ..., p unités de côtés, et cherchons la somme des termes qu'il faut ajouter au cube de rang $(p-1)$ pour obtenir le cube de rang p. Nous trouvons facilement

$$(u_p V_p + v_p U_p - u_p v_p)(W_p - w_p) + w_p U_p V_p.$$

Mais la somme des termes de la Table est égale au produit $U_x V_x W_x$ des sommes des trois suites; on a donc l'identité

$$(2) \quad \left\{ \begin{aligned} & U_x V_x W_x - \sum_{p=1}^{p=x} (u_p V_p W_p + v_p W_p U_p + w_p U_p V_p) \\ & \qquad + \sum_{p=1}^{p=x} (u_p v_p W_p + v_p w_p U_p + w_p u_p V_p) - \sum_{p=1}^{p=x} u_p v_p w_p = 0. \end{aligned} \right.$$

Dans le cas où les trois séries sont identiques, on a

$$U_x^3 - 3\Sigma u_p U_p^2 + 3\Sigma u_p^2 U_p - \Sigma u_p^3 = 0.$$

Par induction, on obtient une formule générale, qui s'applique à un nombre quelconque n de suites, dans laquelle on aperçoit les coefficients du développement de $(1-x)^n$,

$$(3)\qquad U_x^n - C_n^1\,\Sigma u_p U_p^{n-1} + C_n^2\,\Sigma u_p^2 U_p^{n-2} - \ldots + (-1)^n\,\Sigma u_p^n = 0.$$

Exemple I. — Si l'on fait $u_p = 1$ dans la formule précédente, et si l'on remplace x par $(x-1)$, on obtient la formule équivalente au développement de

$$(x-1)^n + (S-1)^n - S^n = 0;$$

cette formule coïncide avec la formule (2) du n° 132.

Exemple II. — Si l'on suppose, dans la formule (1),

$$u_p = v_p = p(p+1)\ldots(p+q-1),$$

on a, par la sommation des factorielles,

$$U_p = \frac{p(p+1)\ldots(p+q)}{q+1},$$

et, par suite,

$$\sum_{p=1}^{p=x}(2p+q-1)u_p^2 = \frac{[x(x+1)\ldots(x+q)]^2}{q+1}.$$

Exemple III. — Si, dans la même formule, on suppose

$$u_p = \frac{1}{p(p+1)},\qquad v_p = a^p,$$

on obtient les relations

$$\sum_{p=1}^{p=x}\frac{a^p}{p(p+1)}[1+(a-1)p^2] = \frac{x}{x+1}a^{x+1},$$

$$\sum_{p=1}^{p=x}\frac{1-(a-1)p}{p(p+1)}a^p = a - \frac{a^{x+1}}{x+1}.$$

En particulier, on fera dans ces formules a égal à $\frac{3}{4}$, $\frac{1}{2}$ ou 2.

140. Développement du produit $S_m S_n$ en fonction linéaire des sommes S. — Dans les formules de ce numéro, S_n désigne d'abord la somme des puissances d'exposant n des x premiers nombres, et l'on suppose $B_1 = +\frac{1}{2}$; d'ailleurs les formules obtenues ne contiendront pas B_1, de telle sorte que les formules auront

lieu, quelle que soit la valeur de x. Faisons, dans la formule (1) du numéro précédent,

$$u_p = p^m, \qquad v_p = p^n,$$

il vient la formule symbolique

$$(1)\quad S_m S_n + S_{m+n} \triangleq S^m \frac{(S+B)^{n+1} - B^{n+1}}{n+1} + S^n \frac{(S+B)^{m+1} - B^{m+1}}{m+1}.$$

Nous avons ainsi exprimé $S_m S_n$ en fonction linéaire des sommes S (nº **102**), et l'on voit que B_1 n'entre pas dans cette formule. En supposant $m = n$, on a

$$(2)\qquad \frac{n+1}{2} S_n^2 = S_{2n+1} + C_{n+1}^2 B_2 S_{2n-1} + C_{n+1}^4 B_4 S_{2n-3} + \ldots$$

Exemple I. — En supposant n égal à $1, 2, 3, 4, \ldots$, on trouve successivement

$$\begin{aligned} S_1^2 &= S_3, \\ S_2^2 &= \tfrac{2}{3} S_5 + \tfrac{1}{3} S_3, \\ S_3^2 &= \tfrac{1}{2} S_7 + \tfrac{1}{2} S_5, \\ S_4^2 &= \tfrac{2}{5} S_9 + \tfrac{2}{3} S_7 - \tfrac{1}{15} S_5, \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

Inversement, on obtient les formules

$$\begin{aligned} 2S_3 &= 2S_1^2, \\ 2S_5 &= 3S_2^2 - S_1^2, \\ 2S_7 &= 4S_3^2 - 3S_2^2 + S_1^2, \\ 2S_9 &= 5S_4^2 - \tfrac{20}{3} S_3^2 + \tfrac{11}{2} S_2^2 - \tfrac{11}{6} S_1^2, \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \end{aligned}$$

Exemple II. — Il résulte immédiatement de la formule de BERNOULLI (nº **134**) que les rapports

$$\frac{S_p}{x} \quad \text{et} \quad \frac{S_{2p-1}}{x^2}$$

ont respectivement pour valeurs

$$B_p \quad \text{et} \quad \frac{2p-1}{2} B_{2p-2},$$

pour $x = 0$. Si l'on introduit ces résultats dans toutes les formules qui

contiennent S, on obtient des formules correspondantes pour les nombres bernoulliens. En particulier, la formule (1) donne

$$B_{m+n} \triangleq B^m \frac{(B+B')^{n+1} - B'^{(n+1)}}{n+1} + B^n \frac{(B+B')^{m+1} - B'^{(m+1)}}{m+1},$$

en supposant $B_1 = 0$. On ne réduit pas les B avec les B'; mais, après le développement du second membre, on remplace les exposants de B et de B' par des indices. Pour $m = 1$ et $n = (2p-1)$, on a

$$(2p-1)B_{2p} + (B+B')^{2p} \triangleq 0.$$

Cette formule donne une relation du second degré entre les nombres de Bernoulli. Elle a été publiée, sans la forme symbolique, par M. Worontzoff, dans les *Nouvelles Annales de Mathématiques* (t. XV, janvier 1876), et par M. Le Paige, dans les *Bulletins de l'Académie de Belgique* (t. XLI, mai 1876).

Exemple III. — Au moyen de la formule (2), on peut exprimer le produit $S_m S_n S_p$ en fonction linéaire des sommes S. On a ainsi, en particulier,

$$4(S_1)^3 = 3S_5 + S_3,$$
$$12(S_2)^3 = 16S_6 - 5S_4 + S_2.$$

Voir dans les *Nouvelles Annales de Mathématiques* (2e série, t. X) un article de M. Amigues.

141. Somme alternée des puissances des nombres entiers. — Si l'on désigne par x un nombre pair, on a les formules

$$p[1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (x-1)^{p-1}] \triangleq (x+B)^p - B^p,$$
$$p\left[1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + \left(\frac{x}{2}-1\right)^{p-1}\right] \triangleq \left(\frac{x}{2}+B\right)^p - B^p.$$

Multiplions par 2^p tous les termes de la seconde égalité, retranchons ensuite de la première, et posons

(1) $$1^{p-1} - 2^{p-1} + 3^{p-1} - \ldots + (x-1)^{p-1} = \Sigma_{p-1},$$

avec

(2) $$2(1-2^p)B_p = G_p;$$

il vient la formule symbolique

(3) $$2p\,\Sigma_{p-1} \triangleq (-1)^x(x+G)^p - G^p.$$

Ainsi, comme dans le développement de S_{p-1}, les coefficients du

développement de Σ_{p-1} sont ceux du binôme multipliés respectivement par les nombres G, qui se déduisent des nombres bernoulliens par la formule (2), ou plus généralement par la formule

$$(2') \qquad \tfrac{1}{2} f(G) \doteq f(B) - f(2B).$$

On a, pour les premières valeurs de p,

$$G_0 = 0, \quad G_1 = +1, \quad G_2 = -1, \quad G_4 = +1,$$
$$G_6 = -3, \quad G_8 = +17, \quad G_{10} = -155, \quad G_{12} = +2073,$$

et G_{2p+1} est nul, de même que B_{2p+1}. Ces nombres ont été considérés par Euler et plus particulièrement par Genocchi ([1]).

Si, dans la formule (3), on remplace x par $(x+2)$, on obtient par différence

$$(x + G + 2)^p - (x + G)^p \doteq -2p[(x+1)^{p-1} - x^{p-1}];$$

cette identité, qui s'applique pour toutes les valeurs paires et positives de x, est vérifiée pour une valeur quelconque entière ou fractionnaire, positive ou négative. Donc, en désignant par $f(x)$ un polynôme quelconque, on a l'*identité fondamentale* pour le calcul des nombres de Genocchi

$$f(x + G + 2) - f(x + G) \doteq -2[f'(x+1) - f'(x)].$$

Avec la notation des différences et des différentielles, on a

$$\Delta f(x + G) \doteq -2\Delta \frac{df}{dx};$$

puis, pour le cas de deux variables,

$$\Delta^2 f(x + G, y + G') \doteq (-2)^2 \Delta^2 \frac{\partial^2 f}{\partial x\, \partial y},$$

en supposant Δx, Δy égaux à 2 dans le premier membre de ces égalités, et égaux à 1 dans le second membre. Cette relation s'étend à un nombre quelconque de variables.

142. Nombres de Genocchi. — Nous avons trouvé au n° 135 (formule 6), la relation

$$f(2B + 1) + f(2B) - 2f(B) \doteq 0;$$

---

(1) *Annales de Tortolini*, t. III. Rome, 1852.

mais, d'autre part, nous avons

$$f(B-1) - f(B) \doteq f'(0);$$

par suite, en retranchant membre à membre,

$$[f(2B-1) - f(B-1)] - [f(2B) - f(B)] \doteq -f'(0).$$

En tenant compte de la définition des nombres G, donnée dans le numéro précédent, on a donc

$$f(G-1) - f(G) \doteq 2f'(0).$$

En particulier, pour $f(x) = x^n$ et $f(x) = (x-1)^m x^m$, il vient, avec $n > 1$,

$$G^1 - (G-1)^1 \doteq 2,$$
$$G^m(G-1)^m - G^m(G-1)^m \doteq 0;$$

pour $m = n > 1$, la formule précédente devient

$$G^n(G-1)^n \doteq 0,$$

car les nombres G sont nuls, comme les nombres B, pour n impair et > 1. Cette formule démontre immédiatement que *les nombres G d'indice pair sont entiers et impairs.*

Soit $F(x)$ le polynôme intégral de $f(x)$, on a

$$F(x+G-1) - F(x+G) \doteq 2f(x);$$

remplaçons successivement x par 0, 1, 2, ..., $(x-1)$ dans l'égalité précédente; faisons la somme alternée des égalités obtenues, il vient

$$[illegible]$$

ce résultat a été indiqué par Euler, qui y est parvenu d'une manière assez pénible (¹).

En posant $f(x) = x^p$, et [illegible]

$$[illegible]$$

il vient

$$[illegible]$$

(¹) Euler, *Traité des différences et des séries* [illegible]

Exemple I. — Calculer les sommes Σ_p pour $p = 0, 1, 2, 3, 4$.

On trouve

$$\begin{aligned} 2\,\Sigma_0 &= (-1)^x - 1, \\ 4\,\Sigma_1 &= (-1)^x(2x+1) + 1, \\ 2\,\Sigma_2 &= (-1)^x(x^2 - x), \\ 8\,\Sigma_3 &= (-1)^x(4x^3 - 4x^2 + 1) - 1, \\ \Sigma_4 &= \Sigma_2(x^2 - x - 1). \end{aligned}$$

143. Somme des puissances des nombres impairs. — Si l'on désigne par T_p l'expression

$$(1) \qquad T_p = 1^p + 3^p + \ldots + (2x-1)^p,$$

on a, pour le nombre impair de rang x,

$$(2x-1)^p = (2x)^p - C_p^1(2x)^{p-1} + C_p^2(2x)^{p-2} + \ldots + (-1)^p;$$

remplaçons successivement x par $1, 2, 3, \ldots, x$, et faisons la somme des égalités obtenues, il vient, en supposant ici que S_p désigne la somme des puissances d'exposant p des x premiers nombres, l'égalité symbolique

$$(2) \qquad T^p \triangleq (2S-1)^p;$$

par suite, les symboles T et $(2S-1)$ et, plus généralement, quelle que soit la valeur de l'indéterminée λ, les symboles $(T+\lambda)$ et $(2S-1+\lambda)$ sont équivalents dans les formules; on peut donc remplacer S par $\frac{1}{2}(T+1)$ dans les formules qui contiennent S. Ainsi, par exemple, on a la formule

$$(3) \qquad f(T+2) - f(T) \triangleq f(2x+1) - f(1).$$

On obtient la somme des puissances semblables T_p des nombres impairs par un polynôme développé suivant les puissances ascendantes de x, au moyen de la remarque suivante, qui était connue des algébristes arabes (¹) : *La somme des puissances $p^{\text{ièmes}}$ des $2x$ premiers nombres entiers égale la somme des puissances $p^{\text{ièmes}}$*

(¹) LACROIX, dans son *Traité de Calcul différentiel*, etc., attribue cette proposition à LORGNA (2ᵉ édition, t. III, p. 445 et 759). On trouve la somme des cubes des nombres impairs dans un ouvrage d'IBN ALMADJDI. Voir les *Annales de Tortolini* (t. VI, p. 239).

des x premiers nombres impairs, augmentée du produit par 2^p de la somme des mêmes puissances des x premiers entiers.

On a donc

$$pT_{p-1} \doteq (2x + B)^p - B^p - 2^{p-1}[(x + B)^p - B^p];$$

par conséquent, si l'on pose

$$(4) \qquad R_p = B_p(1 - 2^{p-1}),$$

on a, pour T_{p-1}, le développement

$$(5) \qquad pT_{p-1} \doteq (2x + R)^p - R^p.$$

Si l'on remplace x par $(x + 1)$ dans la formule (5) et si l'on prend la différence, on obtient l'identité

$$(2x + 2 + R)^p - (2x + R)^p \doteq p(2x + 1)^{p-1};$$

par suite, en remplaçant $(2x + 1)$ par y, il vient

$$(y + R + 1)^p - (y + R - 1)^p \doteq p\, y^{p-1};$$

d'où l'on déduit la relation plus générale

$$f(y + R + 1) - f(y + R - 1) \doteq f'(y),$$

et, en particulier, pour $y = 0$,

$$(6) \qquad f(R + 1) - f(R - 1) \doteq f'(0)\ [1].$$

Cette formule est *l'identité fondamentale* pour le calcul direct des coefficients R, que l'on peut aussi déduire des nombres bernoulliens. Les premières valeurs de R sont, avec $R_{2n+1} = 0$,

$$R_0 = +\frac{1}{2}, \qquad R_2 = -\frac{1}{6}, \qquad R_4 = +\frac{7}{30}, \qquad R_6 = -\frac{31}{42},$$
$$R_8 = +\frac{127}{30}, \qquad R_{10} = -\frac{2555}{66}.$$

---

[1] Si l'on remplace successivement, dans la formule (6), le polynôme $f(x)$ par

$$e^{xz}, \quad \sin xz,$$

on obtient les développements

$$\frac{z}{e^z - e^{-z}} \doteq e^{Rz}, \qquad \frac{z}{2}\,\text{coséc}\, z \doteq \cos Rz,$$

convergents pour toutes les valeurs réelles ou imaginaires de z, dont le module est $< \pi$.

Voir SERRET, *Traité de Trigonométrie*, 5e édition, p. 265 et 31.

Exemple I. — Calculer les sommes T_p des puissances des x premiers nombres impairs, jusqu'à $p = 8$.

Si l'on pose $y = 4x^2$, on trouve pour les exposants impairs

$$
\begin{aligned}
T_1 &= x^2,\\
T_3 &= x^2(\tfrac{1}{2}y - 1),\\
T_5 &= \tfrac{1}{3}x^2(y^2 - 5y + 7),\\
T_7 &= x^2(\tfrac{1}{4}y^3 - \tfrac{7}{3}y^2 + \tfrac{49}{6}y - \tfrac{31}{3}).
\end{aligned}
$$

et pour les exposants pairs

$$
\begin{aligned}
3T_2 &= x(y - 1),\\
5T_4 &= T_2(3y - 7),\\
7T_6 &= T_2(3y^2 - 18y + 31),\\
3T_8 &= T_2(y^3 - 11y^2 + \tfrac{239}{5}y - \tfrac{381}{5})
\end{aligned}
$$

Exemple II. — Démontrer la formule

$$(R + 1)(R + 3)\dots(R + 2p - 1) \triangleq \frac{p}{p+1}\, 2^p . p!$$

Exemple III. — Exprimer T_p en fonction du dernier terme $(2x - 1) = z$. On trouve

$$2p\, T_{p-1} \triangleq (z + 2B)^p - 2R^p.$$

Exemple IV. — Développer le produit $T_m T_n$ en fonction linéaire des sommes T.

Si l'on fait $u_p = (2p - 1)^m$ et $v_p = (2p - 1)^n$ dans la formule (1) du n° 139, il vient, en supposant $B_1 = +\frac{1}{2}$,

$$T_m T_n + T_{m+n} \triangleq T^m \frac{(T + 2B)^{n+1} - 2R^{n+1}}{2n + 2} + T^n \frac{(T + 2B)^{m+1} - 2R^{m+1}}{2m + 2},$$

et, en particulier, pour $m = n$,

$$(T_n)^2 + T_{2n} \triangleq T^n \frac{(T + 2B)^{n+1} - 2R^{n+1}}{n + 1}.$$

Si l'on fait $z = (2x - 1) = 0$, l'expression $2nT_{n-1}$ devient égale à G_n et l'on obtient alors une relation entre les nombres B et G, car les R disparaissent.

144. Sommation alternée des puissances des nombres impairs. — Reprenons l'identité du n° 142

$$(x + G + 1)^n + (x + G)^n \triangleq 2nx^{n-1};$$

remplaçons x par $\frac{1}{2}x$, il vient

$$(x+2G+2)^n - (x+2G)^n \doteq 4nx^{n-1};$$

par suite, en désignant par $f(x)$ un polynôme entier, et par $F(x)$ le polynôme intégral, on a

$$(1) \qquad 4f(x) \doteq F(x+2G+2) - F(x+2G);$$

remplaçons successivement x par 1, 3, 5, ..., $(2x-1)$, et faisons la somme alternée des égalités obtenues, il vient

$$(2) \qquad \begin{cases} f(1) - f(3) + f(5) - \ldots - (-1)^x f(2x-1) \\ \qquad \doteq \frac{1}{4}F(2G+1) - \frac{1}{4}(-1)^x F(2x+2G+1). \end{cases}$$

145. Nombres d'Euler (¹). — Nous appellerons ainsi les nombres définis par la formule de récurrence

$$(1) \qquad (E+1)^p + (E-1)^p \doteq 0,$$

pour toutes les valeurs entières et positives de p, avec la condition $E_0 = 1$, de telle sorte que, pour $p = 0$, on doit remplacer le second membre 0 de la formule précédente par 2. Si l'on désigne par $f(x)$ une fonction entière quelconque, on a donc l'*identité fondamentale*

$$(2) \qquad f(E+1) + f(E-1) \doteq 2f(0);$$

par exemple, pour $f(x) = (x-1)^p(x+1)^q$, il vient

$$(3) \qquad E^p(E+2)^q + E^q(E-2)^p \doteq 2(-1)^p.$$

On a, pour les premières valeurs de l'indice,

$$E_0 = +1, \quad E_2 = -1, \quad E_4 = +5, \quad E_6 = -61,$$
$$E_8 = +1385, \quad E_{10} = -50521, \quad E_{12} = +2702765, \quad \ldots;$$

d'ailleurs, la formule (1) montre immédiatement que $E_{2n+1} = 0$, et que les nombres eulériens d'indice pair sont entiers et impairs.

(¹) SYLVESTER, *Comptes rendus de l'Académie des Sciences* (Paris, t. XXV, p. 161).

La formule (2) peut se généraliser ainsi (n° **121**)

$$(4) \qquad f(x + \mathrm{E} + 1) + f(x + \mathrm{E} - 1) \triangleq 2f(x);$$

remplaçons successivement x par les nombres impairs 1, 3, 5, ..., $(2x - 1)$, et faisons la somme alternée des égalités obtenues, il vient

$$(5) \qquad \begin{cases} f(1) - f(3) + f(5) - \ldots - (-1)^x f(2x - 1) \\ \qquad \triangleq \frac{1}{2} f(\mathrm{E}) - \frac{1}{2}(-1)^x f(2x + \mathrm{E}). \end{cases}$$

Exemple I. — Trouver la somme alternée des puissances semblables des x premiers nombres impairs.

En posant

$$\Theta_p = 1^p - 3^p + 5^p - \ldots + (-1)^{x-1}(2x - 1)^p,$$

on a, en faisant $f(x) = x^p$ dans la formule (5),

$$2\Theta_p \triangleq \mathrm{E}^p - (-1)^x (2x + \mathrm{E})^p.$$

On trouve ainsi, pour les indices impairs, en posant $y = 2x$,

$$\begin{aligned} \Theta_1 &= (-1)^{x-1} x, \\ \Theta_3 &= \Theta_1 (y^2 - 3), \\ \Theta_5 &= \Theta_1 (y^2 - 5)^2, \\ \Theta_7 &= \Theta_1 (y^6 - 21 y^4 + 175 y^2 - 427), \\ \Theta_9 &= \Theta_1 (y^8 - 36 y^6 + 630 y^4 - 5124 y^2 + 12465). \end{aligned}$$

Exemple II. — Démontrer que le quotient de Θ_3 par Θ_1 n'est jamais un carré parfait, et que le quotient de Θ_5 par Θ_1 est un carré parfait et n'est jamais un bicarré.

L'étude de la Table des carrés montre que la différence de deux carrés n'est égale à 3 que pour $(2^2 - 1^2)$ et à 5 que pour $(3^2 - 2^2)$, et puisque l'on a

$$\frac{\Theta_3}{\Theta_1} = 4x^2 - 3, \qquad \frac{\Theta_5}{\Theta_1} = (4x^2 - 5)^2,$$

le théorème est démontré, car on suppose x entier et positif.

146. Relations entre les nombres d'Euler et les nombres de Bernoulli. — En comparant les deux dernières formules des numéros précédents, dont les premiers membres sont identiques, on en déduit la relation générale

$$f(2\mathrm{G} + 1) \triangleq 2f'(\mathrm{E}),$$

et, avec une variable arbitraire (nº **121**),

$$f(z+2G+1) \triangleq 2f'(z+E).$$

On a ainsi une première relation générale entre les nombres d'Euler et ceux de Genocchi. En particulier, pour $f(z)=z^m$, on a la formule

$$(z+2G+1)^m \triangleq 2m(z+E)^{m-1};$$

puis, pour $z=-1$, il vient

$$(2G)^m \triangleq 2m(E-1)^{m-1}$$

et, pour $z=0$,

$$2mE^{m-1} \triangleq (2G+1)^m;$$

ces deux formules ont été obtenues par Scherk [1], mais sans l'emploi du calcul symbolique. Elles expriment les nombres de Genocchi en fonction des nombres d'Euler, et inversement.

147. Formules de Cesàro. — Considérons une suite de nombres

$$a_0, \quad a_1, \quad a_2, \quad \ldots, \quad a_{n-2}, \quad a_{n-1}, \quad a_n,$$

tels que la somme des nombres à égale distance des extrêmes soit constante et égale à x; désignons par S_p la somme de leurs puissances d'exposant p,

$$S_p = a_0^p + a_1^p + a_2^p + \ldots + a_n^p;$$

par hypothèse, nous pouvons encore écrire

$$S_p = (x-a_0)^p + (x-a_1)^p + \ldots + (x-a_n)^p;$$

mais si r représente l'un des nombres $0, 1, 2, \ldots, n$, on a par la formule du binôme

$$(x-a_r)^p = x^p - C_p^1 x^{p-1} a_r + C_p^2 x^{p-2} a_r^2 + \ldots + (-a_r)^p;$$

remplaçons successivement r par $0, 1, 2, \ldots, n$, et faisons la somme des égalités obtenues, nous trouvons la formule symbolique

$$S^p \triangleq (x-S)^p, \tag{1}$$

---

[1] Scherk, *Mathematische Abhandlungen* (Berlin, 1825).

en tenant compte de l'exposant zéro de S. Plus généralement, si l'on désigne par $f(y)$ un polynôme entier, on a l'identité

$$(2) \qquad f(\mathrm{S}) \doteq f(x - \mathrm{S}).$$

Supposons, par exemple, $f(y) = y^p(1 - y)^q$, il vient

$$(3) \qquad \mathrm{S}^p(x - \mathrm{S})^q \doteq \mathrm{S}^q(x - \mathrm{S})^p$$

et, pour $q = (p + 1)$, on a

$$(4) \qquad \mathrm{S}^p(x - \mathrm{S})^p(x - 2\mathrm{S}) \doteq 0.$$

En faisant $p = 1, 2, 3, 4$, on trouve successivement

$$\begin{aligned}
0 &= x^2 \mathrm{S}_1 - 3x \mathrm{S}_2 + 2 \mathrm{S}_3,\\
0 &= x^3 \mathrm{S}_2 - 4x^2 \mathrm{S}_3 + 5x \mathrm{S}_4 - 2 \mathrm{S}_5,\\
0 &= x^4 \mathrm{S}_3 - 5x^3 \mathrm{S}_4 + 9x^2 \mathrm{S}_5 - 7x \mathrm{S}_6 + 2 \mathrm{S}_7,\\
0 &= x^5 \mathrm{S}_4 - 6x^4 \mathrm{S}_5 + 14x^3 \mathrm{S}_6 - 16x^2 \mathrm{S}_7 + 9x \mathrm{S}_8 - 2 \mathrm{S}_9,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Ces formules ne déterminent les sommes S que pour les indices impairs de S, puisque les termes a sont en nombre quelconque et ne sont assujettis qu'aux conditions énoncées plus haut. Mais ces formules s'appliquent évidemment aux sommes S des puissances semblables des x premiers nombres entiers, des puissances semblables des termes d'une progression arithmétique et à beaucoup d'autres suites.

148. Suites de Cesàro. — Nous désignerons, sous ce nom, toute suite de nombres

$$(1) \qquad \mathrm{A}_0, \quad \mathrm{A}_1, \quad \mathrm{A}_2, \quad \ldots, \quad \mathrm{A}_n, \quad \ldots,$$

tels que l'on a pour tout nombre n, entier et positif, la relation symbolique fondamentale

$$(2) \qquad \mathrm{A}^n \doteq (1 - \mathrm{A})^n.$$

En supposant $\mathrm{A}_0 = 1$, on a $\mathrm{A}_1 = \frac{1}{2}$; mais A_2 n'est pas déterminé par l'équation précédente qui ne détermine les nombres A que pour les indices pairs, lorsque l'on connaît les nombres qui correspondent aux indices impairs, ou inversement.

Les formules précédentes permettent de simplifier notablement la théorie des développements en séries des fonctions circulaires et des fonctions exponentielles. En supposant le module de z plus petit que $\frac{1}{2}\pi$, on a les séries convergentes

$$\frac{z}{e^z-1} \triangleq e^{Bz}, \qquad \frac{z}{2}\cot\frac{z}{2} \triangleq \cos Bz,$$

$$\frac{z}{e^z-e^{-z}} \triangleq e^{Rz}, \qquad \frac{z}{2}\operatorname{cos\acute{e}c} z \triangleq \cos Rz,$$

$$\frac{2z}{e^z+1} \triangleq e^{Gz}, \qquad z\operatorname{tang}\frac{z}{2} \triangleq \cos Gz,$$

$$\frac{2}{e^z+e^{-z}} \triangleq e^{Ez}, \qquad \operatorname{s\acute{e}c} z \triangleq \cos Ez.$$

On en déduit les valeurs des séries

$$\frac{1}{1^{2p}} + \frac{1}{2^{2p}} + \frac{1}{3^{2p}} + \frac{1}{4^{2p}} + \ldots = (-1)^{p-1}\frac{2^{2p-1}}{(2p)!}\pi^{2p}B_{2p},$$

$$\frac{1}{1^{2p}} - \frac{1}{2^{2p}} + \frac{1}{3^{2p}} - \frac{1}{4^{2p}} + \ldots = + \frac{1}{(2p)!}\pi^{2p}R_{2p},$$

$$\frac{1}{1^{2p}} + \frac{1}{3^{2p}} + \frac{1}{5^{2p}} + \frac{1}{7^{2p}} + \ldots = (-1)^{p-1}\frac{1}{(2p)!}\pi^{2p}G_{2p},$$

$$\frac{1}{1^{2p}} - \frac{1}{3^{2p}} + \frac{1}{5^{2p}} - \frac{1}{7^{2p}} + \ldots = \frac{(-1)^p}{2^{2p+2}}\frac{\pi}{(2p)!}\pi^{2p}E_{2p}.$$

On peut étendre les formules du texte pour les développements de S_p, T_p, Σ_p, Θ_p, lorsque l'on suppose p positif ou négatif, entier ou fractionnaire; mais les développements sont illimités et conduisent aux définitions des nombres B, R, G, E, d'indice négatif ou fractionnaire. En particulier, pour $p = -1$, on a la formule de STIRLING et la constante d'EULER.

Les développements des puissances $q^{\text{ièmes}}$ des séries

$$e^{Bz}, \quad e^{Rz}, \quad e^{Gz}, \quad e^{Ez},$$

mis sous les formes exponentielles symboliques

$$e^{B_q z}, \quad e^{R_q z}, \quad e^{G_q z}, \quad e^{E_q z},$$

conduisent aux définitions des nombres B, R, G, E des divers ordres.

Voir, pour plus de détails, nos articles du *Bulletin de la Société mathématique* (t. V, VI, VII, VIII).

Exemple I. — Étudier, comme au n° 119, les propriétés des polynômes T_p, Σ_p, Θ_p.

Exemple II. — Appliquer les formules des *Exemples I* et *II* du n° 133 aux nombres R, G, E.

Exemple III. — Donner, pour les sommes alternées, trois formules analogues à la formule (1) du n° 136.

Exemple IV. — Appliquer les théories et les formules du n° 138 à la sommation successive pour les sommes T, Σ, Θ.

Exemple V. — Développer, comme au n° 140, les produits

$$T_m T_n, \quad \Sigma_m \Sigma_n, \quad \Theta_m \Theta_n$$

en fonction linéaire des sommes T, Σ, Θ.

Exemple VI. — Démontrer la formule

$$f(E+2) - f(E-2) \doteq 2f(1) - 2f(-1),$$

et en déduire, pour le calcul rapide des nombres d'Euler, les formules données par M. Radicke,

$$E^m(E+4)^n - E^n(E-4)^m \doteq 2(-1)^m(3^n - 3^m),$$

et

$$\frac{2m+1}{1} E_{2m} + \frac{2m-1}{3} 2^4 C_m^2 E_{2m-2} + \frac{2m-3}{5} 2^8 C_m^4 E_{2m-4} + \ldots = (-3)^m;$$

le dernier terme du premier membre est $2^{2m} E_m$ ou $(m+2) 2^{m-2} E_{m+1}$, suivant que m est pair ou impair.

Exemple VII. — Démontrer la formule

$$E_n \doteq (1+\Delta)\left(1 - \frac{\Delta^2}{2} + \frac{\Delta^4}{2^2} - \frac{\Delta^6}{2^3} + \ldots\right),$$

dans laquelle on remplace les puissances de Δ par les différences correspondantes de x^n pour $x = 0$.

Exemple VIII. — Démontrer que si $f(x)$ désigne un polynôme quelconque, on a les formules

$$hf'(x) \doteq e^{Bhf(x+h)} - e^{Bhf(x)},$$
$$hf'(x) \doteq e^{Rhf(x+h)} - e^{Rhf(x-h)},$$
$$2hf'(x) \doteq e^{Ghf(x+h)} + e^{Ghf(x)},$$
$$2f(x) \doteq e^{Ehf(x+h)} + e^{Ehf(x-h)},$$

en remplaçant, après le développement exponentiel du second membre, les exposants de B, R, G, E par des indices, et les exposants de $f(x)$ de $f(x+h)$ et de $f(x-h)$ par des indices de dérivation. La première et la troisième des formules précédentes correspondent à des développements qui ont été donnés par Euler, par Stirling et par Boole.

CHAPITRE XV.

LES FONCTIONS SYMÉTRIQUES.

150. Fonctions symétriques fondamentales. — On appelle *fonction symétrique* de plusieurs quantités toute fonction qui ne change pas, quand on échange de toutes les manières possibles les quantités qu'elle renferme. Ainsi le produit

$$f(x) = (x-a)(x-b)(x-c)\ldots(x-l)$$

est une fonction symétrique des n quantités $a, b, c, \ldots, l$, quelle que soit la valeur de x. En développant le produit, on trouve

$$f(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \ldots + (-1)^n p_n,$$

en écrivant, suivant l'usage,

$$p_1 = \Sigma a, \quad p_2 = \Sigma ab, \quad p_3 = \Sigma abc, \quad \ldots, \quad p_n = abc\ldots l.$$

Les coefficients $p_1, p_2, p_3, \ldots, p_n$ sont des fonctions symétriques des n quantités; ce sont, en effet, les fonctions symétriques les plus simples, puisque chaque quantité n'y figure qu'au premier degré; nous les appellerons *fonctions symétriques fondamentales*. Lorsque toutes les quantités sont égales, on retrouve pour $f(x)$ le développement du binôme $(x-a)^n$; d'ailleurs, la fonction symétrique fondamentale p_q contient les combinaisons C_n^q des n lettres prises q à q.

La théorie des fonctions symétriques a pour objet principal d'exprimer toutes les fonctions symétriques par les fonctions symétriques fondamentales et, inversement, d'exprimer toute fonction de $p_1, p_2, p_3, \ldots, p_n$, au moyen des quantités $a, b, c, \ldots, l$.

151. Formules de Newton. — Ces formules ont pour objet d'exprimer les sommes des puissances de même exposant des

quantités $a, b, c, \ldots, l$ par les fonctions symétriques fondamentales. Soit

$$s_q = \Sigma a^q = a^q + b^q + c^q + \ldots + l^q;$$

on a l'identité (n° **111**)

$$f'(x) = \frac{f(x)}{x-a} + \frac{f(x)}{x-b} + \frac{f(x)}{x-c} + \cdots + \frac{f(x)}{x-l};$$

mais, en se reportant à l'expression du quotient de $f(x)$ par $(x-a)$ donnée au n° **72**, et en faisant la somme des quotients, on trouve par l'identification

$$(1)\quad \left\{\begin{array}{l} 0 = s_1 \quad - p_1, \\ 0 = s_2 \quad - p_1 s_1 \quad + 2p_2, \\ 0 = s_3 \quad - p_1 s_2 \quad + p_2 s_1 \quad - 3p_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0 = s_{n-1} - p_1 s_{n-2} + p_2 s_{n-3} - \ldots + (-1)^{n-1}(n-1)p_{n-1}. \end{array}\right.$$

La première de ces formules fait connaître s_1, la deuxième s_2, la troisième s_3, et ainsi de suite jusqu'à s_{n-1}. On trouve ainsi

$$(2)\quad \left\{\begin{array}{l} s_1 = p_1, \\ s_2 = p_1^2 - 2p_2, \\ s_3 = p_1^3 - 3p_1 p_2 + 3p_3, \\ s_4 = p_1^4 - 4p_1^2 p_2 + 4p_1 p_3 + 2p_2^2 \quad - 4p_4, \\ s_5 = p_1^5 - 5p_1^3 p_2 + 5p_1^2 p_3 + 5p_1 p_2^2 - 5p_1 p_4 - 5p_2 p_3 + 5p_5, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

Pour obtenir les sommes des puissances dont l'exposant surpasse $(n-1)$, on remarque que $x^q f(x)$ s'annule pour a, b, $c, \ldots, l$, et, par suite, qu'il en est de même de la somme de ces quantités. On a donc la formule générale symbolique

$$s^q f(s) \overset{\wedge}{=} 0,$$

dans laquelle q désigne un nombre entier positif, nul ou négatif. En supposant $q = 1, 2, 3, \ldots$, on calculera successivement $s_n, s_{n+1}, s_{n+2}, \ldots$; en supposant $q = -1, -2, -3, \ldots$, on calculera successivement $s_0, s_{-1}, s_{-2}, \ldots$; on a d'ailleurs $s_0 = n$.

Inversement, on peut calculer les fonctions symétriques fondamentales $p_1, p_2, p_3, \ldots, p_n$, lorsque l'on connaît $s_1, s_2, s_3, \ldots, s_n$.

On a

$$(3)\quad\left\{\begin{array}{l} 1!\,p_1 = s_1,\\ 2!\,p_2 = s_1^2 - \quad s_2,\\ 3!\,p_3 = s_1^3 - \ 3s_1s_2 + \ 2s_3,\\ 4!\,p_4 = s_1^4 - \ 6s_1^2s_2 + \ 8s_1s_3 + \ 3s_2^2 \ - 6s_4,\\ 5!\,p_5 = s_1^5 - 10s_1^3s_2 + 20s_1^2s_3 + 15s_1s_2^2 - 30s_1s_4 - 20s_2s_3 + 24s_5,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right.$$

Exemple I. — On a la formule

$$(\Sigma a^2 + \Sigma ab)^2 = \Sigma a^2(\Sigma a)^2 + (\Sigma ab)^2.$$

Exemple II. — La somme des produits q à q des n quantités

$$a,\ a^2,\ a^3,\ \ldots,\ a^n$$

a pour expression

$$\frac{a^n - 1}{a - 1}\,\frac{a^{n-1} - 1}{a^2 - 1}\,\frac{a^{n-2} - 1}{a^3 - 1}\cdots\frac{a^{n-q+1} - 1}{a^q - 1}\,a^{\frac{q(q+1)}{2}}.$$

Exemple III. — Soient des nombres positifs $a, b, c, \ldots, l$, en nombre p; désignons par A, G, H les moyennes arithmétique, géométrique, harmonique de leurs puissances d'exposant p; si les nombres donnés ne sont pas tous égaux, on a les inégalités (*ordre alphabétique*)

$$A > G > H.$$

En effet, par définition,

$$A = \frac{a^p + b^p + c^p + \ldots + l^p}{p},$$

$$G = abc\ldots l,$$

$$\frac{p}{H} = \frac{1}{a^p} + \frac{1}{b^p} + \frac{1}{c^p} + \ldots + \frac{1}{l^p}.$$

Nous démontrerons d'abord que l'on a $A > G$; en effet, supposons la proposition vérifiée pour $(p - 1)$ nombres; nous allons démontrer qu'elle a lieu encore pour p nombres. On a évidemment

$$(a^{p-1} - b^{p-1})(a - b) \mathrel{\overline{\overline{>}}} 0;$$

d'où l'on déduit

$$a^p + b^p \mathrel{\overline{\overline{>}}} a^{p-1}b + b^{p-1}a.$$

Ajoutons membre à membre toutes les inégalités que l'on peut former

en prenant toutes les combinaisons deux à deux des p nombres, nous obtenons

$$\begin{aligned}(p-1)\Sigma a^p > a(&b^{p-1}+c^{p-1}+\ldots+l^{p-1}),\\ +b(&a^{p-1}+c^{p-1}+\ldots+l^{p-1}),\\ &\ldots\ldots\ldots\ldots\\ +l\,(&a^{p-1}+b^{p-1}+\ldots+k^{p-1}).\end{aligned}$$

Mais, par hypothèse,

$$\begin{aligned}b^{p-1}+c^{p-1}+\ldots+l^{p-1} &> (p-1)\,bc\ldots l,\\ a^{p-1}+c^{p-1}+\ldots+l^{p-1} &> (p-1)\,ac\ldots l,\\ \ldots\ldots\ldots\ldots\ldots\ldots&\ldots\ldots;\end{aligned}$$

par conséquent,

$$(p-1)\,\Sigma a^p > p(p-1)\,abc\ldots l,$$

et, par suite, $A > G$.

En appliquant le résultat précédent aux inverses des nombres a, b, c, ..., l, on trouve ainsi $G > H$.

Exemple IV. - L'expression

$$S_n = (a+b)^n + (-a)^n + (-b)^n$$

est divisible par

$$q = a^2 + ab + b^2,$$

lorsque n est un nombre impair non divisible par 3, et par q^2 lorsque $n = 6m+1$. (CAUCHY.)

En effet, on peut considérer S_n comme la somme des puissances d'exposant n des trois quantités $(a+b)$, $(-a)$, $(-b)$, dont les fonctions symétriques fondamentales sont

$$0, \quad -q, \quad r = ab(a+b).$$

On a donc, sous forme symbolique, la loi de récurrence

$$S^3 \triangleq qS + r;$$

on en déduit

$$(S^3 - r)^3 \triangleq q^3 S^3,$$

et, par le développement,

$$S_9 + (3r^2 - q^3)S_3 = 3rS_6 + r^3.$$

Cette formule permet de calculer les sommes S pour les indices de trois en trois. En élevant les deux membres au carré, on en déduit la relation récurrente symbolique

$$S^{18} - (2q^3 + 3r^2)S^{12} + (q^6 - 6q^3r^2 + 3r^4)S^6 - r_9 S^0 \triangleq 0;$$

cette formule permet de calculer les sommes S pour les indices croissants de six en six, et de vérifier le théorème énoncé.

Exemple V. — Pour n impair et multiple de 3, l'expression

$$(a+b)^n - a^n - b^n - 3(ab)^{\frac{n-1}{2}}(a+b)$$

est divisible par $a^2 + ab^2 + b^2$. (CAUCHY.)

152. Démonstration figurée. — Considérons des pions disposés sur n lignes → et contenant respectivement $a, b, c, d, \ldots$ pions ; ainsi (*fig.* 75) nous avons, par exemple, $a = 5$, $b = 4$, $c = 2$,

Fig. 75.

a	o	o	o	o	o	
b	o	o	o	o		
c	o	o				
d	o	o	o	o	o	o
e	o	o	o			

$d = 6$, $e = 3$. Soit q un nombre entier positif, quelconque, et considérons tous les *arrangements complets* de q pions, à la condition de prendre tous les pions dans une même ligne ; la ligne a renferme a^q arrangements complets ; la ligne b en renferme b^q, et ainsi des autres ; de telle sorte que le tableau renferme

$$S_q = a^q + b^q + c^q + \ldots + l^q$$

arrangements complets. D'autre part, considérons toutes les *combinaisons simples* de tous les pions, en nombre S_1, mais en prenant q pions de telle sorte qu'il n'en soit pris qu'un seul par ligne ; puisqu'on peut choisir entre $a, b, c, \ldots$ pions, dans chaque ligne respective, il est clair que le nombre de ces combinaisons est égal à la fonction symétrique fondamentale

$$p_q = \Sigma_q\, abc \ldots .$$

Nous allons calculer S_q en fonction de S_{q-1}, S_{q-2}, ... Pour former les arrangements complets S_q, nous prenons d'abord tous les arrangements complets $(q-1)$ à $(q-1)$, en nombre S_{q-1},

et nous ajoutons un quelconque des $S_1 = p_1$ pions. Nous formons ainsi

$$p_1 S_{q-1}$$

dispositions ; mais nous avons compté en trop les arrangements dans lesquels le pion ajouté appartient à une ligne différente de l'arrangement S_{q-1}. Mais pour former les arrangements complets contenant $(q-1)$ pions dans une ligne et un dans une autre, on peut partir de tous les arrangements complets S_{q-2} ; les systèmes des deux lignes occupées par les pions sont en nombre p_2, et l'on a ainsi $p_2 S_{q-2}$ dispositions ; on aurait donc

$$p_1 S_{q-1} - p_2 S_{q-2}.$$

Mais, parmi les dernières dispositions, on a compté en trop celles qui contiennent $(q-2)$ pions dans une ligne et deux pions dans deux autres lignes différentes ; on a donc

$$p_1 S_{q-1} - p_2 S_{q-2} + p_3 S_{q-3},$$

et ainsi de suite. Enfin, les dernières dispositions obtenues, en nombre $p_{q-1} S_1$, ne sont pas précisément celles que l'on devait obtenir ; nous avons compté en trop toutes les dispositions de q éléments, pris sur q lignes différentes, en nombre p_q ; de plus, toutes ces combinaisons ont été comptées q fois, car pour les obtenir nous avons pris une combinaison de $(q-1)$ pions, et nous en avons ajouté un autre. On a donc la formule générale (¹)

$$S_q - p_1 S_{q-1} + p_2 S_{q-2} - p_3 S_{q-3} + \ldots \pm p_{q-1} S_1 \mp p_q . q = 0.$$

Cette formule renferme toutes les formules de NEWTON, car on peut supposer $q > n$, et alors $p_q = 0$.

153. Fonctions symétriques doubles, triples. — Nous venons d'indiquer la méthode de calcul des fonctions symétriques simples, c'est-à-dire des fonctions dont chaque terme ne contient qu'une seule quantité ; on appelle *fonctions symétriques doubles, triples, ...* celles dont chaque terme contient deux, trois, ... lettres.

(¹) MANTEL, *Sur les combinaisons d'éléments disperses dans un plan* (Congrès de Rouen, 1883). — *Voir* aussi le n° 81.

Si l'on suppose $\alpha \gtrless \beta$, on a

$$\Sigma a^\alpha b^\beta = s_\alpha s_\beta - s_{\alpha+\beta};$$

le nombre des termes de Σ est le nombre A_n^2 des arrangements simples de n objets pris deux à deux. Mais, si l'on suppose $\alpha = \beta$, on a

$$2\Sigma a^\alpha b^\alpha = s_\alpha^2 - s_{2\alpha},$$

et le nombre des termes de Σ est la moitié de A_n^2.

Si l'on suppose α, β, γ inégaux deux à deux, on a

$$\Sigma a^\alpha b^\beta c^\gamma = s_\alpha s_\beta s_\gamma - s_\alpha s_{\beta+\gamma} - s_\beta s_{\gamma+\alpha} - s_\gamma s_{\alpha+\beta} + 2 s_{\alpha+\beta+\gamma};$$

le nombre des termes de la fonction symétrique triple est égal au nombre A_n^3 des arrangements simples de n objets pris trois à trois. Mais si deux exposants deviennent égaux, on doit diviser le second membre par $2!$ et si les trois exposants deviennent égaux, on doit diviser par $3!$

On peut calculer ainsi successivement les fonctions multiples $\Sigma a^\alpha b^\beta \ldots l^\lambda$; le nombre des termes de cette fonction est égal au nombre des permutations avec répétition des exposants α, β, γ, ..., λ, entiers, positifs ou nuls.

Lorsque tous les exposants des lettres de la fonction symétrique sont égaux, le calcul se simplifie, puisque cela revient à remplacer les quantités a, b, c, ..., l par a^α, b^α, c^α, ..., l^α; par suite, les formules (3) du n° **151** donnent

$$\begin{aligned}
2!\,\Sigma(ab)^\alpha &= s_\alpha^2 - s_{2\alpha},\\
3!\,\Sigma(abc)^\alpha &= s_\alpha^3 - 3 s_\alpha s_{2\alpha} + 2 s_{3\alpha},\\
4!\,\Sigma(abcd)^\alpha &= s_\alpha^4 - 6 s_\alpha^2 s_{2\alpha} + 8 s_\alpha s_{3\alpha} + 3 s_{2\alpha}^2 - 6 s_{4\alpha},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

154. Rangement et nombre des termes d'une fonction symétrique entière. — Considérons une fonction entière et symétrique F des lettres a, b, c, ..., l; désignons par α le plus grand exposant. A cause de la symétrie, la fonction F contient a^α et si nous mettons a^α en facteur dans tous les termes qui le contiennent, on a

$$F = a^\alpha F_1 + \ldots,$$

et F_1 est une fonction symétrique des $(n-1)$ lettres $b, c, \ldots, l$. Désignons par β le plus grand exposant dans F_1, il est au plus égal à α, et l'on peut poser

$$F_1 = b^\beta F_2 + \ldots,$$

F_2 étant une fonction symétrique des $(n-2)$ lettres $c, d, \ldots, l$. Et ainsi de suite, de telle sorte que le premier terme de F est

$$A a^\alpha b^\beta c^\gamma \ldots l^\lambda,$$

A désignant une constante et $\alpha, \beta, \gamma, \ldots, \lambda$ des nombres positifs non croissants, les derniers pouvant être nuls. Si l'on désigne par G la fonction symétrique formée en permutant tous les exposants du terme précédent, la différence $(F-G)$ sera une fonction symétrique dont on déterminera de même le premier terme

$$A_1 a^{\alpha_1} b^{\beta_1} c^{\gamma_1} \ldots l^{\lambda_1},$$

A_1 désignant une constante et $\alpha_1, \beta_1, \gamma_1, \ldots, \lambda_1$ des entiers non croissants, positifs ou nuls, c'est-à-dire tels que les différences

$$\alpha_1 - \beta_1, \quad \beta_1 - \gamma_1, \quad \gamma_1 - \delta_1, \quad \ldots, \quad \varkappa_1 - \lambda_1$$

ne soient pas négatives. Et ainsi de suite.

D'ailleurs le nombre des termes de la fonction symétrique générale et homogène de degré μ est égal au nombre des termes du développement de

$$(a + b + c + \ldots + l)^\mu,$$

c'est-à-dire à D_n^μ; si la fonction n'est pas homogène, le nombre des termes est égal à D_{n+1}^μ (*voir* le n° 80).

155. Méthode de Waring. — On a

$$\begin{aligned} p_1 &= \Sigma a, \\ p_2 &= \Sigma ab, \\ p_3 &= \Sigma abc, \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ p_n &= abc\ldots l; \end{aligned}$$

élevons les deux membres de ces égalités aux puissances d'exposants

$$\alpha - \beta, \quad \beta - \gamma, \quad \gamma - \delta, \quad \ldots, \quad \varkappa - \lambda, \quad \lambda;$$

multiplions membre à membre, et par A. Le produit

$$A p_1^{\alpha-\beta} p_2^{\beta-\gamma} p_3^{\gamma-\delta} \ldots p_{n-1}^{\varkappa-\lambda} p_n^{\lambda}$$

est une fonction symétrique que nous désignerons par W et dont le premier terme est égal au premier terme de F. Le calcul de F est ainsi ramené au calcul de la fonction symétrique (F — W) que l'on range suivant l'ordre indiqué; on opère sur (F — W), comme sur F, et l'on trouve une nouvelle fonction W_1 égale à

$$A_1 p_1^{\alpha_1-\beta_1} p_2^{\beta_1-\gamma_1} p_3^{\gamma_1-\delta_1} \ldots p_{n-1}^{\varkappa_1-\lambda_1} p_n^{\lambda_1};$$

on opère de même sur $(F - W - W_1)$, et ainsi de suite. Finalement on a

$$F = W + W_1 + W_2 + \ldots$$

et la fonction F se trouve exprimée en fonction des coefficients p par un nombre d'opérations qui ne surpasse pas le nombre des termes de la fonction symétrique générale.

Par suite, on a ce théorème important : Toute fonction symétrique entière et à coefficients entiers de n quantités $a, b, c, \ldots, l$ s'exprime par une fonction entière, à coefficients entiers, des fonctions symétriques fondamentales.

156. Degré et poids d'une fonction symétrique. — Désignons encore par

$$A a^{\alpha} b^{\beta} c^{\gamma} \ldots l^{\lambda}$$

le premier terme d'une fonction symétrique; il résulte immédiatement de la théorie précédente que cette fonction est de *degré* α par rapport à $p_1, p_2, p_3, \ldots, p_n$, puisqu'elle contient le terme

$$(1) \qquad A p_1^{\alpha-\beta} p_2^{\beta-\gamma} p_3^{\gamma-\delta} \ldots p_{n-1}^{\varkappa-\lambda} p_n^{\lambda},$$

de degré

$$(\alpha-\beta)+(\beta-\gamma)+(\gamma-\delta)+\ldots+(\varkappa-\lambda)+\lambda = \alpha.$$

Ainsi le terme de plus haut degré de la fonction F, exprimée au moyen des fonctions symétriques fondamentales, est égal à α.

On appelle *poids* d'un terme par rapport à des quantités $p_1, p_2, p_3, \ldots, p_n$, affectées d'indices, la somme des produits obtenus en

multipliant l'exposant de chaque lettre par son indice; ainsi le poids du terme (1) est

$$1(\alpha-\beta)+2(\beta-\gamma)+\ldots+(n-1)(\varkappa-\lambda)+n\lambda,$$

c'est-à-dire

$$\alpha+\beta+\gamma+\ldots+\varkappa+\lambda=\mu.$$

Par suite, toute fonction symétrique et homogène de degré μ de n quantités $a, b, c, \ldots, l$ est une fonction entière de degré α par rapport à $p_1, p_2, p_3, \ldots, p_n$, et dont tous les termes sont du même poids μ. On peut vérifier directement ce théorème en observant que, si l'on multiplie toutes les quantités données par un même nombre quelconque t, la fonction symétrique homogène se trouve multipliée par t^μ et les fonctions symétriques fondamentales $p_1, p_2, p_3, \ldots, p_n$ sont respectivement multipliées par $t, t^2, t^3, \ldots, t^n$.

A l'aide des deux principes précédents, on peut écrire immédiatement la partie littérale d'une fonction symétrique, et il ne reste à déterminer que les coefficients. Ainsi la fonction

$$\Sigma a^2(b-c)^2$$

est de degré 2 et de poids 4; par conséquent, les seuls termes qu'elle peut contenir sont p_4, p_3p_1, p_2^2.

Exemple I. — Calculer l'expression de Σa^3b^2c.

On trouve

$$p_1p_2p_3-3p_1^2p_4-3p_3^2+4p_2p_4+7p_1p_5-12p_6.$$

Exemple II. — On a les formules

$$\Sigma a^\alpha b^\alpha(a-b)^2=s_\alpha s_{\alpha+2}-s_{\alpha+1}^2,$$
$$\Sigma a^\alpha b^\alpha(a+b)(a-b)^2=s_\alpha s_{\alpha+3}-s_{\alpha+1}s_{\alpha+2}.$$

Exemple III. — Calculer les valeurs des fonctions symétriques Σa^2b^2, $\Sigma a^2b^2c^2, \ldots$.

En désignant par μ le nombre des carrés contenus dans chaque terme, on a, pour Σ_μ, l'expression

$$p_\mu^2-2p_{\mu-1}p_{\mu+1}+2p_{\mu-2}p_{\mu+2}-\ldots\pm 2p_1p_{2\mu-1}\mp 2p_{2\mu}.$$

157. Formules de Waring. — On peut calculer directement s_α au moyen des fonctions symétriques fondamentales par une formule

de WARING. On peut démontrer de diverses manières (¹) que s_α est le produit de α par le coefficient de $x^{-\alpha}$ dans le développement de l'expression

$$R + \frac{R^2}{2} + \frac{R^3}{3} + \ldots + \frac{R^\alpha}{\alpha},$$

en supposant

$$R = \frac{p_1}{x} - \frac{p_2}{x^2} + \frac{p_3}{x^3} - \ldots - (-1)^n \frac{p_n}{x^n}.$$

Par suite, on a

$$(1) \qquad s_\alpha = \sum \alpha \frac{(\lambda_1 + \lambda_2 + \ldots + \lambda_r - 1)!}{\lambda_1!\,\lambda_2!\,\lambda_3!\ldots\lambda_r!} p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_r^{\lambda_r},$$

et le signe Σ s'étend à toutes les valeurs entières, positives ou nulles, des λ qui vérifient la relation

$$\lambda_1 + 2\lambda_2 + \ldots + r\lambda_r = \alpha.$$

Inversement, on peut calculer les fonctions symétriques fondamentales $p_1, p_2, p_3, \ldots, p_n$, au moyen des sommes $s_1, s_2, s_3, \ldots, s_n$; on démontre que $(-1)^\alpha p_\alpha$ est égal au coefficient de x^α dans le développement de l'expression

$$1 - \frac{Q}{1!} + \frac{Q^2}{2!} - \frac{Q^3}{3!} + \ldots + (-1)^\alpha \frac{Q^\alpha}{\alpha!},$$

en supposant

$$Q = \frac{s_1}{x} + \frac{s_2}{2x^2} + \frac{s_3}{3x^3} + \ldots + \frac{s_n}{nx^n} + \ldots;$$

(¹) La méthode la plus rapide, qui ne peut trouver sa place dans le texte, repose sur l'identité

$$\left(1 - \frac{a}{x}\right)\left(1 - \frac{b}{x}\right)\ldots\left(1 - \frac{l}{x}\right) = 1 - \frac{p_1}{x} + \frac{p_2}{x^2} - \ldots + (-1)^n \frac{p_n}{x^n};$$

si l'on prend les logarithmes des deux membres, on en déduit l'identité

$$Q \triangleq \frac{s_1}{x} + \frac{s_2}{2x^2} + \ldots + \frac{s_\alpha}{\alpha x^\alpha} + \ldots \triangleq -\log(1 - R);$$

et si l'on développe le second membre en série, il suffit d'égaler les coefficients de $x^{-\alpha}$.

Inversement, on a l'identité symbolique

$$1 - R \triangleq e^{Q},$$

qui donne les formules suivantes.

par suite, on a

$$(2)\qquad (-1)^{\alpha} p_{\alpha} = \sum \frac{(-1)^{\lambda_1+\lambda_2+\ldots+\lambda_r}}{\lambda_1!\,\lambda_2!\ldots\lambda_r!}\left(\frac{s_1}{1}\right)^{\lambda_1}\left(\frac{s_2}{2}\right)^{\lambda_2}\cdots\left(\frac{s_r}{r}\right)^{\lambda_r},$$

et le signe Σ s'étend à toutes les valeurs entières, positives ou nulles, des λ qui vérifient la relation

$$\lambda_1 + 2\lambda_2 + \ldots + r\lambda_r = \alpha.$$

Exemple I. — En particulier, les fonctions symétriques de deux quantités a et b, pour lesquelles

$$a + b = p, \qquad ab = q, \qquad a^n + b^n = s_n,$$

sont données par la formule

$$s_n = p^n - \frac{n}{1!} p^{n-2} q + \frac{n(n-3)}{2!} p^{n-4} q^2 - \ldots$$
$$+ (-1)^r \frac{n(n-r-1)(n-r-2)\ldots(n-2r+1)}{r!} p^{n-2r} q^r + \ldots.$$

Si l'on remplace a par x, b par x^{-1}, p par y et q par 1, on exprime $X_n = x^n + x^{-n}$ en fonction de $y = x + x^{-1}$.

Exemple II. — En reprenant les notations de l'Exemple IV (n° 151), on a encore la formule

$$(a+b)^n - a^n - b^n = nqr\left[q^{n-3} - \frac{n-3}{2!} q^{n-5} r + \frac{(n-4)(n-5)}{3!} q^{n-7} r^2 - \ldots\right].$$

Exemple III. — Avec les mêmes notations, la première formule de Waring montre que s_α est le produit de α par le coefficient de $x^{-\alpha}$ dans le développement de l'expression

$$R + \frac{R^2}{2} + \frac{R^3}{3} + \ldots + \frac{R^\alpha}{\alpha},$$

en supposant

$$R = \frac{1}{x}\left(q - \frac{r}{x}\right);$$

on a donc

$$s_{2n} = 2n \sum \frac{C_{n-i}^{2i}}{n-i} q^{n-3i} r^{2i},$$

$$s_{2n+1} = (2n+1) \sum \frac{C_{n-i}^{2i+1}}{n-i} q^{n-3i-1} r^{2i+1},$$

pour toutes les valeurs entières de i non négatives, pour lesquelles les exposants de q et de r ne sont pas négatifs.

On en déduit immédiatement, en posant

$$s_n = (a+b)^n + (-a)^n + (-b)^n,$$
$$q = a^2 + ab + b^2,$$
$$r = ab(a+b),$$

que si

$n = 6m$,	s_n n'est divisible ni par q, ni par r;
$n = 6m+1$,	s_n est divisible par $q^2 r$;
$n = 6m+2$,	s_n » » » q, et non par r;
$n = 6m+3$,	s_n » » » r, » » » q;
$n = 6m+4$,	s_n » » » q^2, » » » r;
$n = 6m+5$,	s_n » » » qr.

FONCTIONS DE DIFFÉRENCES.

158. Formules de Lagrange. — Elles servent à exprimer les sommes des puissances de même exposant des différences mutuelles de n quantités données, au moyen des sommes des puissances de ces quantités elles-mêmes. Désignons encore par a, b, c, ..., l les n quantités données; par S_α la somme des puissances d'exposant α de leurs $n(n-1)$ différences mutuelles. Lorsque α est impair, la somme S_α est nulle, puisque les termes tels que $(a-b)^\alpha$ et $(b-a)^\alpha$ sont égaux et de signes contraires; mais, si α est pair, ces termes s'ajoutent et l'on remplace S_α par $2\,S\frac{\alpha}{2}$, en ne considérant alors que les carrés des différences, au nombre de

$$\nu = \tfrac{1}{2}n(n-1).$$

On a, par la formule du binôme,

$$\Sigma(x-a)^{2q} = s_0 x^{2q} - C_{2q}^1 s_1 x^{2q-1} + C_{2q}^2 s_2 x^{2q-2} + \ldots + s_{2q};$$

si l'on remplace successivement x par a, b, c, ..., l, et si l'on fait la somme des résultats, on obtient

$$S_q = s_0 s_{2q} - C_{2q}^1 s_1 s_{2q-1} + C_{2q}^2 s_2 s_{2q-2} - \ldots + \tfrac{1}{2}(-1)^q C_{2q}^q s_q s_q.$$

En donnant à q les valeurs successives des ν premiers entiers, on calculera S_1, S_2, S_3, ..., S_ν. Par les formules de Newton, ou par celles de Waring, on pourra calculer les fonctions symétriques

fondamentales $P_1, P_2, P_3, \ldots, P_\nu$ des carrés des différences des n quantités données, au moyen des fonctions symétriques fondamentales $p_1, p_2, p_3, \ldots, p_n$ de ces quantités elles-mêmes.

On suivrait une marche semblable pour former les fonctions symétriques des sommes des n quantités données prises deux à deux.

Exemple I. — Si l'on désigne par p, q, r les fonctions symétriques fondamentales de trois quantités, et par P, Q, R les fonctions symétriques fondamentales des carrés de leurs différences, on a d'abord

$$\begin{aligned}
s_1 &= p,\\
s_2 &= p^2 - 2q,\\
s_3 &= p^3 - 3pq + 3r,\\
s_4 &= p^4 - 4p^2q + 4pr + 2q^2\\
s_5 &= p^5 - 5p^3q + 5p^2r + 5pq^2 - 5qr,\\
s_6 &= p^6 - 6p^4q + 6p^3r + 9p^2q^2 - 12pqr - 2q^3 + 3r^2;
\end{aligned}$$

puis, par les formules de LAGRANGE,

$$\begin{aligned}
S_1 &= 3s_2 - s_1^2,\\
S_2 &= 3s_4 - 4s_1s_3 + 3s_2^2,\\
S_3 &= 3s_6 - 6s_1s_5 + 15s_2s_4 - 10s_3^2
\end{aligned}$$

et, par suite,

$$\begin{aligned}
S_1 &= 2p^2 - 6q,\\
S_2 &= 2p^4 - 12p^2q + 18q^2,\\
S_3 &= 2p^6 - 18p^4q - 12p^3r + 57p^2q^2 + 54pqr - 66q^3 - 81r^2;
\end{aligned}$$

enfin, par les formules (2) du n° 151

$$\begin{aligned}
P &= 2p^2 - 6q,\\
Q &= p^4 - 6p^2q + 9q^2,\\
R &= p^2q^2 + 18pqr - 4q^3 - 4p^3r - 27r^2.
\end{aligned}$$

159. Méthode de Serret. — Toute fonction des différences de n quantités ne change pas, lorsqu'on augmente celles-ci d'un même nombre t; alors les fonctions symétriques fondamentales prennent des accroissements

$$\Delta p_1, \quad \Delta p_2, \quad \ldots, \quad \Delta p_{n-1}, \quad \Delta p_n,$$

qui s'annulent avec t, et dont les termes qui contiennent t à la première puissance sont respectivement

$$nt, \quad (n-1)p_1 t, \quad \ldots, \quad 2p_{n-2}t, \quad p_{n-1}t.$$

Mais une fonction quelconque φ de $p_1, p_2, \ldots, p_{n-1}, p_n$ devient

$$\varphi(p_1 + \Delta p_1, p_2 + \Delta p_2, \ldots);$$

puisque le résultat ne change pas pour une fonction de différences, les coefficients des diverses puissances de t, et en particulier celui de t, sont nuls. Par conséquent, la fonction φ doit vérifier la relation

$$n\frac{\partial\varphi}{\partial p_1} + (n-1)p_1\frac{\partial\varphi}{\partial p_2} + (n-2)p_2\frac{\partial\varphi}{\partial p_3} + \ldots = 0.$$

Exemple I. — Former le produit φ des carrés des différences de trois quantités données a, b, c, au moyen des fonctions symétriques fondamentales

$$p, q, r.$$

La fonction symétrique cherchée est de degré 4, de poids 6; son premier terme est a^4b^2, et ainsi la fonction contient le terme p^2q^2. Soit donc

$$\varphi = p^2q^2 + Ar^2 + Bpqr + Cp^3r + Dq^3;$$

si l'on annule identiquement l'expression

$$3\frac{\partial\varphi}{\partial p} + 2p\frac{\partial\varphi}{\partial q} + q\frac{\partial\varphi}{\partial r},$$

on en tire

$$2A + 3B = 0, \qquad 2B + 9C = 0, \qquad B + 6D + 6 = 0, \qquad C + 4 = 0$$

et, par suite

$$C = -4, \qquad B = +18, \qquad A = -27, \qquad D = -4.$$

160. Fonction alternée de Vandermonde. — On appelle *fonction alternée* de n quantités données toute fonction qui change de signe, mais non de valeur absolue, lorsque l'on échange de toutes les manières possibles, en nombre $\nu = C_n^2$, les quantités qu'elle renferme.

Désignons par V le produit des ν différences des n quantités prises dans l'ordre suivant, déterminé de telle sorte que l'on prend

l'excès de chacune des quantités sur toutes celles qui les précèdent dans l'ordre donné

$$(1)\qquad V = \left\{\begin{array}{l}(b-a)\\(c-a)(c-b)\\(d-a)(d-b)(d-c)\\\dots\dots\dots\dots\dots\\\dots\dots\dots\dots\dots\dots;\\(l-a)(l-b)(l-c)\dots(l-k);\end{array}\right.$$

le produit V est une fonction alternée des n quantités, que l'on appelle la *fonction alternée fondamentale de* VANDERMONDE; en d'autres termes, si l'on échange deux des quantités f et h, par exemple, le produit V change de signe. En effet, V contient quatre groupes de facteurs :

1° Ceux qui ne contiennent ni f, ni h;

2° Ceux qui contiennent f et non h;

3° Ceux qui contiennent h et non f;

4° Le facteur $(f-h)$ ou $(h-f)$.

Les facteurs du premier groupe ne changent pas; ceux du second se transforment en ceux du troisième et inversement; enfin le dernier facteur, seul, change de signe.

Si l'on pose

$$f(x)=(x-a)(x-b)(x-c)\dots(x-l),$$

on a

$$\begin{array}{l}f'(a)=\quad\star\quad(a-b)(a-c)\dots(a-l),\\f'(b)=(b-a)\quad\star\quad(b-c)\dots(b-l),\\f'(c)=(c-a)(c-b)\quad\star\quad\dots(c-l),\\\dots\dots\dots\dots\dots\dots\dots,\\\dots\dots\dots\dots\dots\dots\dots,\\f'(l)=(l-a)(l-b)(l-c)\dots\quad\star\quad;\end{array}$$

par suite, en multipliant,

$$V^2=(-1)^\nu f'(a)f'(b)f'(c)\dots f'(l).$$

Ainsi V^2 est une fonction symétrique des quantités $a, b, c, \dots, l$; il en est de même du carré de toute fonction alternée.

Considérons maintenant une fonction entière quelconque, mais alternée F, des n quantités; le rapport F:V ne change pas par une

transposition de deux quantités; c'est donc une fonction symétrique. Ainsi toute fonction entière et alternée de n quantités est le produit d'une fonction symétrique entière par la fonction alternée fondamentale de VANDERMONDE.

161. Développement de la fonction de Vandermonde. — Si l'on effectue le produit V et qu'on opère la réduction des termes semblables, on obtient un polynôme homogène de degré ν par rapport aux quantités $a, b, c, \ldots, l$. En faisant d'abord le produit des termes de la dernière ligne, puis de la précédente, et ainsi de suite, on voit que V contient le terme

$$a^0 b^1 c^2 d^3 \ldots l^{n-1},$$

avec le coefficient $+1$; c'est le *terme principal* de la fonction alternée; par suite, le produit V est la somme des termes, en nombre $n!$,

$$V = \Sigma \pm a^0 b^1 c^2 \ldots l^{n-1},$$

que l'on peut déduire, du terme principal, par tous les échanges de deux lettres quelconques; ces termes ont le coefficient $+1$, ou -1, suivant qu'ils se déduisent du terme principal par un nombre pair ou impair d'échanges. En effet, la somme Σ est une fonction alternée des n quantités données : elle est donc divisible par V; mais, puisque ces fonctions sont du même degré, le quotient est une constante que l'on trouve égale à l'unité par la considération du terme principal.

On doit observer que, au lieu d'exécuter les permutations sur les lettres $a, b, c, \ldots, l$, on peut, sans changer les résultats, les exécuter sur les indices $0, 1, 2, \ldots, (n-1)$.

CHAPITRE XVI.

LES DÉTERMINANTS.

La résolution du système de deux et de trois équations littérales du premier degré, à deux et à trois inconnues, a conduit Leibniz (1693) à la théorie des déterminants par l'étude de la loi de formation et des propriétés du dénominateur commun des inconnues. En 1750, cette théorie a été retrouvée et généralisée par Cramer, pour la résolution d'un système de n équations littérales du premier degré à n inconnues. Elle fut ensuite appliquée dans un grand nombre de questions d'Analyse par Bézout, Vandermonde, Lagrange, Gauss, Wronski. C'est en 1812 que cette doctrine est devenue féconde, et a été étudiée d'une façon systématique par Cauchy. Elle a été développée considérablement par Jacobi, Cayley, Hesse, Sylvester, Hermite, Clebsch et Borchardt.

Cette théorie a conduit Vandermonde à la notion des *fonctions alternées* dont nous avons donné les principales propriétés dans le Chapitre précédent; inversement, on peut déduire les propriétés générales des déterminants, par l'emploi du calcul symbolique, de la fonction alternée fondamentale de Vandermonde.

« Qu'est-ce au fond, dit Sylvester, que la théorie des déterminants? C'est une Algèbre au-dessus de l'Algèbre, un calcul qui nous met à même de combiner et de prédire les résultats des opérations algébriques, de la même manière que l'Algèbre nous permet de nous dispenser de l'exécution des opérations particulières de l'Arithmétique. »

Dans ce Chapitre, nous exposerons rapidement les principales propriétés de cette théorie, en renvoyant aux Traités spéciaux publiés par Brioschi, Baltzer, Salmon et Günther. Pour le lecteur

peu familiarisé avec cette méthode, nous recommandons plus particulièrement l'Ouvrage de M. MANSION (¹).

162. Définition et propriétés du déterminant. — Désignons par a le symbole de n quantités données

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},$$

par $b, c, \ldots, l$ les symboles d'autres quantités; en d'autres termes, considérons les n^2 quantités quelconques

$$\begin{array}{ccccc} a_0 & b_0 & c_0 & \ldots & l_0 \\ a_1 & b_1 & c_1 & \ldots & l_1 \\ a_2 & b_2 & c_2 & \ldots & l_2 \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ a_{n-1} & b_{n-1} & c_{n-1} & \ldots & l_{n-1} \end{array}$$

Si l'on fait le développement de la fonction alternée fondamentale

$$V = \Sigma \pm a^0 b^1 c^2 \ldots l^{n-1}$$

et si l'on remplace les exposants par des indices, on obtient le *déterminant* ou la *somme alternée*

$$D = \Sigma \pm a_0 b_1 c_2 \ldots l_{n-1}$$

des n^2 quantités données. Comme les échanges nécessaires pour former les termes de V ou de D peuvent porter indifféremment sur les lettres ou sur les indices, on en conclut qu'*un déterminant ne change pas de valeur lorsqu'on remplace les colonnes par les lignes*, car le terme principal formé par le produit des éléments de la diagonale descendante reste le même.

Il résulte de la définition qu'*un déterminant change de signe lorsqu'on échange les éléments de deux colonnes*, puisque cela revient à l'échange de deux lettres de V. Il en est de même dans l'échange de deux lignes. Par suite, *un déterminant qui contient deux rangées identiques est nul.*

(¹) P. MANSION, *Éléments de la théorie des déterminants, avec de nombreux exercices*, 4ᵉ édition; 1883 (Paris, chez Gauthier-Villars).

Il résulte encore du développement de la fonction alternée V que celle-ci se trouve multipliée par λ, lorsqu'on remplace a, b ou c par $a\lambda$, $b\lambda$, $c\lambda$; par suite, *on multiplie ou l'on divise un déterminant par* λ, *en multipliant ou en divisant tous les éléments d'une rangée par* λ. De là ce corollaire :

Un déterminant est nul lorsque les éléments d'une même rangée sont proportionnels aux éléments d'une rangée parallèle.

Enfin, on remarquera que si l'on a

$$a_p = a^p, \qquad b_p = b^p, \qquad c_p = c^p, \qquad \ldots, \qquad l_p = l^p$$

pour toutes les valeurs $0, 1, 2, \ldots, (n-1)$ de p, le déterminant D est identique à la fonction alternée fondamentale.

163. Développement du déterminant. — Le déterminant D est une fonction linéaire et homogène des n quantités

$$a_0, \quad a_1, \quad a_2, \quad \ldots, \quad a_{n-1},$$

et l'on peut poser

$$D = a_0 A_0 + a_1 A_1 + a_2 A_2 + \ldots + a_{n-1} A_{n-1},$$

en désignant par

$$A_0, \quad A_1, \quad A_2, \quad \ldots, \quad A_{n-1}$$

des quantités qui ne contiennent aucun des éléments a. Il est facile de déterminer le coefficient A_0 de a_0, puisqu'il correspond à l'ensemble des termes indépendants de a dans le développement de la fonction V, c'est-à-dire au produit de $bcd\ldots l$ par la fonction alternée fondamentale des lettres $b, c, d, \ldots, l$, en ayant soin de remplacer ensuite les exposants par des indices. On a donc

$$A_0 = \begin{vmatrix} b_1 & c_1 & \ldots & l_1 \\ b_2 & c_2 & \ldots & l_2 \\ \cdot & \cdot & \ldots & \cdot \\ b_{n-1} & c_{n-1} & \ldots & l_{n-1} \end{vmatrix}.$$

Ainsi le coefficient de a_0 dans le déterminant D est égal au déterminant obtenu en supprimant la ligne et la colonne qui contiennent a_0. On peut obtenir de même le coefficient d'un élément

quelconque, dans le développement du déterminant D, suivant tous les éléments d'une même rangée; il est égal au déterminant $\pm$ D', obtenu en supprimant dans le déterminant D la ligne et la colonne qui contiennent cet élément. En effet, sans changer la valeur absolue de D, on peut amener la ligne qui contient l'élément considéré à la place de la ligne supérieure par des échanges consécutifs de deux lignes; on peut ensuite amener la colonne qui contient l'élément considéré, à la place de la première colonne à gauche, par des échanges consécutifs de colonnes. Alors l'élément considéré occupe la place de a_0, et, si l'on supprime la première ligne et la première colonne du déterminant transformé, on obtient le déterminant D'.

Pour déterminer le signe, il suffit d'observer que D a changé autant de fois de signe qu'il y a d'unités, moins deux, dans la somme des rangs de la ligne et de la colonne qui contiennent l'élément considéré. Si l'on suppose les éléments du déterminant placés sur les cases d'un échiquier à deux couleurs alternées, comme l'échiquier ordinaire, on prendra le signe $+$, ou le signe $-$, suivant que l'élément a_0 et l'élément considéré seront placés sur des cases de même couleur, ou sur des cases de couleurs différentes.

Le coefficient d'un élément, pris avec son signe, s'appelle le *mineur* correspondant du premier ordre; on le désigne par une grande lettre. Par suite, un déterminant est égal à la somme des produits obtenus en multipliant tous les éléments d'une même ligne ou d'une même colonne par les mineurs correspondants.

Ainsi, pour le déterminant D du troisième ordre

$$D = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix},$$

on a les six développements

$$\begin{aligned} D &= a_1 A_1 + a_2 A_2 + a_3 A_3, & D &= a_1 A_1 + b_1 B_1 + c_1 C_1, \\ D &= b_1 B_1 + b_2 B_2 + b_3 B_3, & D &= a_2 A_2 + b_2 B_2 + c_2 C_2, \\ D &= c_1 C_1 + c_2 C_2 + c_3 C_3, & D &= a_3 A_3 + b_3 B_3 + c_3 C_3. \end{aligned}$$

161. Calcul des déterminants. — Si tous les éléments d'une rangée d'un déterminant sont nuls, à l'exception d'un seul, le

calcul de D se réduit à celui d'un déterminant ayant une ligne et une colonne en moins.

Si tous les éléments d'une rangée se décomposent en la somme de deux autres, le déterminant se décompose en une somme de deux déterminants.

Un déterminant ne change pas de valeur si l'on ajoute à tous les éléments d'une même rangée ceux d'une autre rangée parallèle multipliés par un même nombre.

Si p lignes ou p colonnes d'un déterminant deviennent identiques pour $x = a$, le déterminant est divisible par $(x - a)^{p-1}$.

Exemple I. — On a

$$\begin{vmatrix} (b+c)^2 & a^2 & a^2 \\ b^2 & (c+a)^2 & b^2 \\ c^2 & c^2 & (a+b)^2 \end{vmatrix} = 2abc(a+b+c)^3.$$

Exemple II. — Le déterminant

$$\begin{vmatrix} (x+2a)^3 & (x+2b)^3 & (x+2c)^3 \\ (x+a)^3 & (x+b)^3 & (x+c)^3 \\ a^3 & b^3 & c^3 \end{vmatrix}$$

est égal au produit de

$$3x^3(b-a)(c-a)(c-b),$$

par

$$(a+b+c)x^2 + 3(bc+ca+ab)x + 6abc.$$

Exemple III. — On a

$$\begin{vmatrix} 0 & a & b & c \\ a & 0 & \gamma & \beta \\ b & \gamma & 0 & \alpha \\ c & \beta & \alpha & 0 \end{vmatrix} = a^2\alpha^2 + b^2\beta^2 + c^2\gamma^2 - 2bc\beta\gamma - 2ca\gamma\alpha - 2ab\alpha\beta.$$

Exemple IV. — On a

$$\begin{vmatrix} x & a & b & c \\ -a & x & \gamma & \beta \\ -b & -\gamma & x & \alpha \\ -c & -\beta & -\alpha & x \end{vmatrix} = x^4 + (a^2 + b^2 + c^2 + \alpha^2 + \beta^2 + \gamma^2)x^2 + (a\alpha + b\beta + c\gamma)^2.$$

Exemple V. — Le déterminant

$$\begin{vmatrix} 0 & 1 & 1 & 1 \\ 1 & a+x & b+x & c+x \\ 1 & a'+y & b'+y & c'+y \\ 1 & a''+z & b''+z & c''+z \end{vmatrix}$$

est indépendant de x, y, z. (SYLVESTER.)

Exemple VI. — Le déterminant à n lignes

$$\begin{vmatrix} a & \lambda & \lambda & \lambda & \dots \\ \mu & b & \lambda & \lambda & \dots \\ \mu & \mu & c & \lambda & \dots \\ \mu & \mu & \mu & d & \dots \\ . & . & . & . & \dots \end{vmatrix},$$

dans lequel tous les éléments d'un même côté de la diagonale sont égaux, a pour expression

$$(-1)^n \frac{\lambda f(\mu) - \mu f(\lambda)}{\lambda - \mu},$$

si l'on pose

$$f(x) = (x-a)(x-b)\dots(x-l).$$

Pour $\mu = \lambda$, il se réduit à

$$(-1)^n [f(\lambda) - \lambda f'(\lambda)].$$

Exemple VII. — Calculer le déterminant

$$\Delta_p = \begin{vmatrix} 1 & 1 & \dots & 1 \\ A_{n+1}^1 & A_{n+2}^1 & \dots & A_{n+p}^1 \\ A_{n+1}^2 & A_{n+2}^2 & \dots & A_{n+p}^2 \\ . & . & \dots & . \\ A_{n+1}^{p-1} & A_{n+2}^{p-1} & \dots & A_{n+p}^{p-1} \end{vmatrix},$$

dans lequel A_p^q désigne le nombre des arrangements simples de p objets pris q à q (n° 45).

Exemple VIII. — Si l'on désigne par $a, b, c, \dots, l$ des quantités quelconques en nombre n, par s leur somme, et par A, B, C, ..., L les excès de cette somme sur les quantités données, le déterminant

$$\begin{vmatrix} x-A & b & c & \dots & l \\ a & x-B & c & \dots & l \\ a & b & x-C & \dots & l \\ . & . & . & \dots & . \\ a & b & c & \dots & x-L \end{vmatrix}$$

a pour expression $x(x-s)^{n-1}$, et le déterminant obtenu en remplaçant $a, b, c, \ldots, l$ par A, B, C, …. L a pour expression

$$[x-(n-2)s](x-s)^{n-1}.$$

Exemple IX. — Le déterminant

$$\begin{vmatrix} a_1-b_1 & a_1-b_2 & \ldots & a_1-b_n \\ a_2-b_1 & a_2-b_2 & \ldots & a_2-b_n \\ a_3-b_1 & a_3-b_2 & \ldots & a_3-b_n \\ \cdot & \cdot & \ldots & \cdot \\ a_n-b_1 & a_n-b_2 & \ldots & a_n-b_n \end{vmatrix}$$

est identiquement nul.

Exemple X. — Le déterminant obtenu en remplaçant les éléments du déterminant précédent par leurs inverses est égal au produit des différences mutuelles des nombres a, multiplié par le produit des différences mutuelles des nombres b et divisé par le produit de toutes les différences telles que (a_r-b_s). (CAUCHY.)

165. Éléments à deux indices. — Au lieu de désigner les éléments d'un déterminant par des lettres différentes (nº 162), on peut se servir d'une seule lettre a avec deux indices, en représentant par a_x^y le terme placé dans la ligne → de rang x et dans la colonne ↓ de rang y.

$$(\text{A})\qquad \begin{array}{l|lllll} a & & & & & y\\ \hline & a_1^1 & a_1^2 & a_1^3 & \ldots & a_1^n, \\ & a_2^1 & a_2^2 & a_2^3 & \ldots & a_2^n, \\ & a_3^1 & a_3^2 & a_3^3 & \ldots & a_3^n, \\ & \cdot & \cdot & \cdot & \ldots & \cdot \\ & a_n^1 & a_n^2 & a_n^3 & \ldots & a_n^n. \\ x & & & & & \end{array}$$

Un terme quelconque du déterminant est donné par

$$\varepsilon a_{x_1}^{y_1} a_{x_2}^{y_2} a_{x_3}^{y_3} \ldots a_{x_n}^{y_n};$$

les nombres $x_1, x_2, x_3, \ldots, x_n$ représentent une permutation quelconque des n premiers nombres, et les nombres $y_1, y_2, y_3, \ldots, y_n$ représentent une permutation quelconque des n premiers nom-

bres; de plus, le coefficient ε est égal à $+1$ ou à -1 suivant que les permutations

$$x_1\, x_2\, x_3 \ldots x_n \quad \text{et} \quad y_1\, y_2\, y_3 \ldots y_n$$

appartiennent à la même classe ou à des classes différentes.

On obtient tous les termes du déterminant, en nombre $n!$, en laissant invariables tous les indices inférieurs x et en permutant de toutes les manières les indices supérieurs y, ou encore en laissant invariables les indices supérieurs y, et en permutant de toutes les manières les indices inférieurs x.

Si l'on change les signes de tous les éléments situés dans les colonnes de rang pair, puis si l'on change les signes de tous les éléments situés dans les lignes de rang pair, la valeur du déterminant reste la même, mais tous les éléments dont la somme des indices est impaire se trouvent, en signe contraire, dans le nouveau déterminant.

Désignons le déterminant des n^2 éléments a par

$$A = \Sigma \pm a_1^1 a_2^2 \ldots a_n^n$$

et par A_r^s le coefficient de a_r^s dans le développement de A, suivant les éléments de la $r^{\text{ième}}$ ligne ou de la $s^{\text{ième}}$ colonne; le mineur du premier ordre, obtenu en supprimant la ligne et la colonne correspondantes, a pour expression $(-1)^{r+s} A_r^s$, et les sommes

$$\begin{gathered} a_r^1 A_s^1 + a_r^2 A_s^2 + \ldots + a_r^n A_s^n, \\ a_1^s A_1^r + a_2^s A_2^r + \ldots + a_n^s A_n^r, \end{gathered}$$

sont égales à A, ou à zéro, suivant que r et s sont égaux ou inégaux.

Si l'on désigne par A, B, P trois déterminants de degré n, formés avec des éléments quelconques a, b, p, à deux indices, le déterminant de degré $2n$

$$C = \begin{vmatrix} a_1^1 & \ldots & a_1^n & p_1^1 & \ldots & p_1^n \\ \cdot & \ldots & \cdot & \cdot & \ldots & \cdot \\ a_n^1 & \ldots & a_n^n & p_n^1 & \ldots & p_n^n \\ 0 & \ldots & 0 & b_1^1 & \ldots & b_1^n \\ \cdot & \ldots & \cdot & \cdot & \ldots & \cdot \\ 0 & \ldots & 0 & b_n^1 & \ldots & b_n^n \end{vmatrix}$$

dans lequel tous les éléments situés au-dessous du déterminant A sont nuls, est égal au produit AB.

Si, pour simplifier, nous posons

$$C = \begin{vmatrix} A & P \\ O & B \end{vmatrix}, \quad C' = \begin{vmatrix} O & B \\ A & P \end{vmatrix},$$

on a $C' = (-1)^n AB$, puisque l'on passe du déterminant C au déterminant C′, en échangeant respectivement les n premières lignes avec les n dernières.

166. Multiplication des déterminants. — Pour multiplier deux déterminants A et B, que l'on peut toujours supposer du même ordre n, nous remplaçons dans le déterminant P tous les éléments de la diagonale principale par -1 et tous les autres par 0; on a donc

$$AB = \begin{vmatrix} a_1^1 & \ldots & a_1^n & (-1) & \ldots & 0 \\ . & \ldots & . & . & \ldots & . \\ a_n^1 & \ldots & a_n^n & 0 & \ldots & (-1) \\ 0 & \ldots & 0 & b_1^1 & \ldots & b_1^n \\ . & \ldots & . & . & \ldots & . \\ 0 & \ldots & 0 & b_n^1 & \ldots & b_n^n \end{vmatrix}$$

Ajoutons aux éléments de la première colonne les éléments des n dernières, multipliés respectivement par

$$a_1^1, a_1^2, a_1^3, \ldots, a_1^n;$$

ajoutons aux éléments de la seconde colonne les éléments des n dernières, multipliés respectivement par

$$a_2^1, a_2^2, a_2^3, \ldots, a_2^n,$$

et ainsi de suite jusqu'à la $n^{\text{ième}}$ colonne. Posons, de plus,

$$c_r^s = a_r^1 b_s^1 + a_r^2 b_s^2 + \ldots + a_r^n b_s^n,$$

le déterminant AB devient

$$\begin{vmatrix} 0 & \ldots & 0 & (-1) & \ldots & 0 \\ . & \ldots & . & . & \ldots & . \\ 0 & \ldots & 0 & 0 & \ldots & (-1) \\ c_1^1 & \ldots & c_1^n & b_1^1 & \ldots & b_1^n \\ . & \ldots & . & . & \ldots & . \\ c_n^1 & \ldots & c_n^n & b_n^1 & \ldots & b_n^n \end{vmatrix}$$

Par suite, d'après la valeur du déterminant C', considéré dans le numéro précédent, on a

$$AB = \Sigma \pm c_1^1 c_2^2 c_3^3 \dots c_n^n.$$

C'est dans cette dernière égalité que consiste la règle de *multiplication par lignes*. En changeant, dans l'un ou l'autre des deux déterminants A et B, les colonnes en lignes ou les lignes en colonnes, on obtient quatre manières de faire la multiplication.

Plus généralement, si l'on considère deux systèmes A et B de qn quantités a et b à deux indices, renfermés dans deux rectangles de q lignes et de n colonnes, et si l'on détermine c_r^s comme ci-dessus, le déterminant des n^2 quantités

$$C = \begin{vmatrix} c_1^1 & \dots & c_1^n \\ . & \dots & . \\ . & \dots & . \\ c_n^1 & \dots & c_n^n \end{vmatrix}$$

est nul pour $n > q$; pour $n = q$, on a $C = AB$, et pour $n < q$, le déterminant C est égal à la somme des produits des déterminants formés en prenant les q colonnes de A et les q colonnes correspondantes de B; le nombre de ces produits est égal au nombre des combinaisons simples de n objets pris q à q. Ce théorème fondamental, donné par Binet et par Cauchy, est la généralisation de résultats qui avaient été obtenus par Lagrange et par Gauss.

Exemple I. — Déterminant symétrique. — C'est un déterminant dans lequel les éléments de la diagonale principale sont quelconques, les éléments placés symétriquement par rapport à cette diagonale étant égaux.

Les mineurs qui correspondent à deux éléments symétriques sont égaux.

Le carré d'un déterminant est un déterminant symétrique.

Carré du déterminant de Vandermonde. — Si l'on pose

$$s_r = a^r + b^r + c^r + \dots + l^r,$$

on a

$$V^2 = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ . & . & . & \dots & . \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}.$$

Exemple II. — *Déterminant gauche.* — C'est un déterminant dans lequel les éléments de la diagonale principale sont quelconques, les éléments placés symétriquement, par rapport à cette diagonale, étant égaux et de signes contraires. Si les éléments de la diagonale principale sont tous nuls, le déterminant est dit *symétrique gauche*.

Si l'on change tous les signes des éléments d'un déterminant symétrique gauche de degré n, on le multiplie par $(-1)^n$; donc il est nul, pour n impair. Les mineurs qui correspondent à des éléments placés symétriquement par rapport à la diagonale sont égaux et de signes contraires.

Un déterminant symétrique gauche de degré pair est le carré d'une fonction de ses éléments, que l'on appelle *Pfaffien*. (CAYLEY.)

Lorsqu'un déterminant symétrique gauche de degré $2n$ est symétrique par rapport à sa seconde diagonale, on peut le mettre sous la forme du carré d'un déterminant de degré n en ajoutant aux éléments d'une rangée ceux de la rangée symétrique par rapport au centre. (GÜNTHER.)

Exemple III. — *Circulant.* — C'est un déterminant dont les lignes successives sont formées par les permutations circulaires des éléments de la première ligne.

Tout circulant de degré pair peut être rendu symétrique par rapport au centre.

Le circulant dont la première ligne se compose de n termes en progression arithmétique de raison r et de somme S a pour expression

$$(-1)^{\frac{n(n-1)}{2}} n^{n-2} r^{n-1} S.$$

Le circulant dont la première ligne se compose des carrés des n premiers nombres entiers a pour expression

$$(-1)^{n-1} \frac{(n+1)(2n+1)n^{n-2}}{12} [(n+2)^n - n^n].$$

Le circulant dont la première ligne se compose des n coefficients du développement de $(1+x)^n$ est égal à 2^n ou à 0, suivant que n est pair ou impair.

Le produit de deux circulants de même degré est un circulant.

ÉQUATIONS DU PREMIER DEGRÉ.

167. Formules de Cramer. — Résolution de deux équations du premier degré à deux inconnues. — Système de trois équations à trois inconnues, de quatre équations à quatre inconnues.

Un système de n équations du premier degré à n inconnues,

dont le déterminant des coefficients des inconnues n'est pas nul, admet une solution et n'en admet qu'une seule. Chacune des inconnues est égale à une fraction ayant pour dénominateur commun le déterminant des coefficients et pour numérateur le déterminant obtenu en remplaçant dans le dénominateur la colonne des coefficients de l'inconnue considérée par les seconds membres des équations.

Pour démontrer ce théorème important, on range les équations de telle sorte que le mineur obtenu en supprimant la première ligne et la première colonne du déterminant ne soit pas nul, et l'on fait voir que le système a une solution unique, en supposant le théorème vérifié pour un système de $(n-1)$ équations à $(n-1)$ inconnues. D'ailleurs, pour chaque colonne du déterminant, il existe un mineur du premier ordre qui n'est pas nul ; par conséquent, les inconnues se présentent toutes sous la forme de Cramer, sans qu'il soit nécessaire de vérifier *a posteriori* l'exactitude du résultat, ainsi que Gauss le pensait.

Exemple I. — Deux marchands de vins entrent dans Paris, l'un avec 64 barriques et l'autre avec 20 barriques du même prix. Mais, comme ils n'ont pas assez d'argent pour acquitter les droits d'entrée, le premier paye avec 5 barriques et ajoute 40^{fr} ; l'autre acquitte avec 2 barriques et on lui rend 40^{fr}. Quels sont les prix de la barrique et du droit d'entrée de chacune d'elles ?

La barrique vaut 110^{fr} et le droit d'entrée est de 10^{fr}. On doit remarquer que les barriques qui restent à l'octroi ne payent pas l'entrée, et c'est là la curiosité de ce problème que Le Verrier appelait *problème piège*.

Exemple II. — Les aiguilles d'une montre sont en coïncidence à midi ; à quels instants seront-elles encore en coïncidence ?

Dans l'intervalle de douze heures, il y a onze rencontres se succédant à un onzième d'heure. — Calcul des éclipses. — Durée de la rotation du soleil autour de son axe, etc.

Exemple III. — Les aiguilles d'une montre sont en coïncidence à midi ; à quels instants seront-elles : 1° directement opposées ; 2° perpendiculaires ; 3° à quels instants sont-elles inclinées d'une fraction donnée du cadran ?

Exemple IV. — Les aiguilles d'une montre sont en coïncidence à midi, quelles sont leurs positions simultanées pour lesquelles les deux aiguilles peuvent être remplacées l'une par l'autre, à un autre instant.

En imaginant une aiguille fictive marchant douze fois plus vite que l'ai-

guille des minutes, les positions demandées se succèdent aux intervalles des temps de coïncidence de l'aiguille des heures et de l'aiguille fictive. Donc, en douze heures, il y a 143 positions des aiguilles, qui se succèdent à intervalles égaux, en tenant compte des coïncidences. — L'énoncé et la solution de ce problème sont dus à M. LAISANT.

Exemple V. — Un paquebot met à la voile de Douvres avec un vent frais, arrive à Calais en deux heures. Pour retourner, le vent étant contraire, il fait 6 milles de moins à l'heure; mais, à mi-chemin, le vent change de nouveau, le paquebot fait deux milles en plus, à l'heure, et revient à Douvres dans les six septièmes du temps qu'il aurait employé si le vent n'avait pas changé. Trouver la distance de Douvres à Calais et les vitesses différentes du paquebot.

Distance, 22 milles. — Vitesses à l'heure, 11,5 et 7 milles.

Exemple VI. — Deux stations distantes de 4^{km} sont reliées par une double ligne de tramways. A chaque station, les voitures partent de trois en trois minutes, et marchent avec la même vitesse sur chaque ligne. Un piéton parcourt uniformément la même ligne; au moment où il part de la première station, il voit une voiture la quitter, une autre y arriver. De même, au moment où il atteint la seconde station, une voiture en part et une autre y arrive. En comptant les voitures avec lesquelles il s'est trouvé à l'une et à l'autre station, le piéton en a rencontré 19 allant dans le même sens et 43 allant en sens contraire. Trouver la vitesse du piéton et celle des voitures?

Exemple VII. — Résoudre les équations

$$\begin{aligned} ax + by + cz + dt &= X, \\ -bx + ay + dz - ct &= Y, \\ -cx - dy + az + bt &= Z, \\ -dx + cy - bz + at &= T. \end{aligned}$$

Si l'on forme le carré du déterminant des inconnues, on voit que ce déterminant est le carré de l'expression

$$\Delta = a^2 + b^2 + c^2 + d^2.$$

On a ensuite

$$\begin{aligned} \Delta x &= aX - bY - cZ - dT, \\ \Delta y &= bX + aY - dZ + cT, \\ \Delta z &= cX + dY + aZ - bT, \\ \Delta t &= dX - cY + bZ + aT, \end{aligned}$$

et, en ajoutant les carrés (n° 69),

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = X^2 + Y^2 + Z^2 + T^2$$

Exemple VIII. — Résoudre, par rapport à x, y, z, t, p, q, r, s, les équations

$$\begin{aligned}
ax + by + cz + dt + ep + fq + gr + hs &= X,\\
-bx + ay - dz - ct + fp - eq + hr + gs &= Y,\\
-cx + dy + az + bt - gp + hq - er - fs &= Z,\\
-dx + cy + bz - at + hp - gq + fr - es &= T,\\
ex - fy + gz - ht - ap + bq + cr + ds &= P,\\
-fx - ey + hz + gt - bp + aq - dr - cs &= Q,\\
-gx + hy + ez - ft + cp + dq - ar - bs &= R,\\
-hx + gy + fz + et + dp - cq + br + as &= S.
\end{aligned}$$

En prenant le carré du déterminant des inconnues, on voit que ce déterminant est le bicarré de l'expression

$$\Delta = a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2.$$

En multipliant ensuite les équations par les nombres a, b, c, d, e, f, g, h, pris avec des signes convenables, on trouve

$$\begin{aligned}
\Delta x &= aX - bY - cZ - dT - eP - fQ + gR - hS,\\
\Delta y &= bX + aY - dZ + cT - fP + eQ + hR - gS,\\
\Delta z &= cX + dY + aZ - bT - gP + hQ + eR + fS,\\
\Delta t &= dX - cY + bZ + aT - hP + gQ - fR + eS,\\
\Delta p &= eX + fY + gZ + hT + aP + bQ - cR - dS,\\
\Delta q &= fX + eY - hZ + gT + bP + aQ + dR - cS,\\
\Delta r &= gX + hY - eZ + fT + cP - dQ + aR + bS,\\
\Delta s &= hX + gY + fZ + eT + dP + cQ + bR + aS.
\end{aligned}$$

En ajoutant les carrés, on démontre que

$$\Sigma a^2 . \Sigma x^2 = \Sigma X^2,$$

ou, en d'autres termes, que *le produit d'une somme de huit carrés par une somme de huit carrés est une somme de huit carrés.*

Exemple IX. — Si la somme des carrés des éléments de chaque ligne d'un déterminant est égale à 1, et qu'en outre la somme des produits des éléments correspondants de deux lignes quelconques soit nulle, les mêmes relations ont lieu entre les éléments des colonnes. — Le déterminant est égal à ± 1, chaque mineur est égal, en valeur absolue, à l'élément correspondant. Enfin, si l'on fait pour chaque ligne le produit des éléments, la somme des carrés de ces produits est égale à la somme correspondante pour les colonnes.

Les trois exemples précédents trouvent leur application dans la théorie

des *carrés magiques*, et inversement cette théorie donne lieu à de nombreuses identités.

168. Théorème de M. Rouché ([1]). — Lorsque le déterminant des coefficients des inconnues est nul, la résolution d'un système linéaire donne lieu à une discussion intéressante qui s'applique à un nombre quelconque p d'équations du premier degré contenant un nombre quelconque q d'inconnues. On forme le Tableau rectangulaire, à p lignes et q colonnes, des coefficients des inconnues, et l'on suppose que l'un au moins des éléments du Tableau n'est pas nul. Alors il existe un déterminant formé avec les coefficients de n lignes et de n colonnes, de telle sorte que ce déterminant de degré n ne soit pas nul, mais tel que tout déterminant de degré $(n+1)$, formé avec les éléments du Tableau, soit identiquement nul. D'ailleurs, il peut exister plusieurs déterminants de degré n qui ne soient pas nuls, et l'on peut choisir l'un d'eux, que l'on appelle *déterminant principal* du système, de telle sorte qu'en modifiant l'ordre des équations et celui des inconnues ce déterminant Δ soit formé des éléments contenus dans les n premières lignes et les n premières colonnes du Tableau.

On borde ensuite le déterminant Δ avec une ligne formée par les éléments correspondants d'une autre ligne du Tableau et avec une colonne contenant les termes connus des équations correspondantes. On obtient ainsi des déterminants, de degré $(n+1)$, que l'on appelle *déterminants caractéristiques* du système linéaire. Cela posé, on a le théorème suivant :

Pour que la résolution d'un système de p équations du premier degré à q inconnues soit possible, il faut et il suffit que tous les déterminants caractéristiques que l'on peut déduire du déterminant principal soient nuls. Lorsque ces conditions sont remplies, le système est déterminé ou indéterminé, suivant que le nombre des inconnues égale ou surpasse le degré du déterminant principal.

Il résulte de ce théorème que la condition nécessaire et suffisante pour qu'un système de n équations à n inconnues admette

([1]) E. Rouché, *Note sur les équations linéaires* (*Journal de l'École Polytechnique*, XLVIII[e] Cahier; 1880).

une solution unique est que le déterminant du système soit différent de o.

REMARQUE I. — La théorie précédente permet de représenter les résultats des opérations fondamentales de l'Arithmétique et de l'Algèbre sous la forme de déterminants. En effet, ces opérations déterminent en général, d'une façon unique, par des équations linéaires, les coefficients de certains polynômes. On peut donc mettre sous forme de déterminant la valeur numérique d'un polynôme, les coefficients du produit ou du quotient de deux polynômes, les coefficients du reste de la division d'un polynôme par un autre polynôme, les coefficients de la formule d'interpolation de LAGRANGE, etc.

REMARQUE II. — Les formules concernant les suites récurrentes donnent encore l'expression des inconnues sous forme de déterminant. Ainsi les formules de la théorie des combinaisons, celles du calcul symbolique, les formules de sommation des puissances numériques, celles qui concernent les nombres de BERNOULLI, d'EULER, de GENOCCHI, les formules de NEWTON sur le calcul des fonctions symétriques, etc., produisent des déterminants. Cependant, il est bon d'observer qu'il ne faut pas abuser de cette forme plus complexe, et surtout lorsque le calcul direct des inconnues est plus rapide que celui que l'on peut obtenir par le développement des déterminants qui leur correspondent.

Exemple I. — Résoudre les équations

$$\frac{x}{a+\lambda} + \frac{y}{b+\lambda} + \frac{z}{c+\lambda} = 1,$$
$$\frac{x}{a+\mu} + \frac{y}{b+\mu} + \frac{z}{c+\mu} = 1,$$
$$\frac{x}{a+\nu} + \frac{y}{b+\nu} + \frac{z}{c+\nu} = 1.$$

Exemple II. — Résoudre les équations

$$\begin{aligned} x + y + z + t &= e_0, \\ ax + by + cz + dt &= e_1, \\ a^2x + b^2y + c^2z + d^2t &= e_2, \\ a^3x + b^3y + c^3z + d^3t &= e_3. \end{aligned}$$

Exemple III. — Trouver, par la théorie des déterminants et par le binôme de LEIBNIZ, la formule qui donne la dérivée d'ordre n d'une fraction $(u : v)$.

169. Équations linéaires et homogènes. — Lorsque les termes qui ne contiennent pas les inconnues sont tous nuls, tous les déterminants caractéristiques sont nuls, puisqu'ils renferment une colonne de zéros; par conséquent, tout système d'équations linéaires et homogènes admet toujours une solution, celle dans laquelle toutes les inconnues sont nulles. Mais on dit que le système des équations est *compatible,* lorsqu'il admet une solution dans laquelle l'une, au moins, des inconnues n'est pas nulle; alors on a deux cas à distinguer, suivant que le degré du déterminant principal est égal au nombre des inconnues, ou se trouve plus petit. Lorsque le degré du déterminant principal est égal au nombre des inconnues, le système n'admet que des valeurs nulles pour les inconnues. Mais, si le nombre des inconnues surpasse, de k unités, le degré du déterminant principal, on peut donner à k des inconnues des valeurs arbitraires et, par suite, différentes de zéro.

Ainsi, *pour qu'un système linéaire et homogène soit compatible, il faut et il suffit que le degré du déterminant principal soit plus petit que le nombre des inconnues.*

En particulier, pour qu'un système de n équations homogènes à n inconnues soit nul, il faut et il suffit que le déterminant des coefficients des inconnues soit nul.

On en déduit diverses propriétés des déterminants identiquement nuls.

Pour qu'un déterminant soit nul, il faut et il suffit qu'il existe entre les éléments des rangées une même relation linéaire et homogène.

Dans un déterminant nul, les mineurs des éléments de deux rangées parallèles sont proportionnels.

170. Formes linéaires et homogènes. — Pour qu'une forme linéaire et homogène soit nulle, quelles que soient les valeurs attribuées aux variables, il faut et il suffit que tous ses coefficients soient nuls.

On dit que des formes linéaires sont *indépendantes* lorsqu'elles

peuvent prendre des valeurs données arbitrairement pour certaines valeurs des variables.

Le nombre des formes homogènes et indépendantes de n variables ne peut surpasser le nombre n des variables.

Pour que n formes homogènes à n variables soient indépendantes, il faut et il suffit que le déterminant des coefficients des variables ne soit pas nul.

Pourque p formes à $(p+q)$ variables soient indépendantes, il faut et il suffit que l'on puisse former avec le Tableau des coefficients des variables un déterminant de degré p qui ne soit pas nul.

CHAPITRE XVII.

LES SUITES RÉCURRENTES LINÉAIRES.

---

171. Des suites récurrentes proprement dites. — On appelle ainsi une suite de nombres

$$\ldots,\quad u_{-3},\quad u_{-2},\quad u_{-1},\quad u_0,\quad u_1,\quad u_2,\quad u_3,\quad \ldots,$$

tels qu'il existe une même *relation linéaire homogène, à coefficients constants,* entre p nombres consécutifs. En d'autres termes, on a dans toute l'étendue de la suite

$$a_0 u_{n+p} + a_1 u_{n+p-1} + \ldots + a_n u_p = 0,$$

ou, sous la forme symbolique,

$$u^p f(u) \triangleq 0,$$

$f(u)$ désignant un polynôme de degré n dont les coefficients extrêmes ne sont pas nuls, et p un entier quelconque. Le polynôme

$$f(u) = a_0 u^n + a_1 u^{n-1} + \ldots + a_n,$$

s'appelle l'*échelle de récurrence*.

Pour une même échelle, il existe une infinité de suites; mais toute suite est déterminée, et peut être prolongée indéfiniment dans les deux sens, lorsque l'on connaît n termes consécutifs et les coefficients de l'échelle. Il résulte immédiatement de là que l'échelle d'une série récurrente ne change pas lorsque l'on augmente d'un même nombre tous les indices des termes et que deux suites de même échelle de degré n sont identiques, si n termes consécutifs sont égaux chacun à chacun.

Lorsque n termes consécutifs d'une suite sont nuls, tous les termes sont nuls; ainsi, une suite illimitée de zéros forme une suite récurrente d'échelle quelconque. Inversement, lorsqu'une

suite récurrente contient n termes consécutifs égaux à zéro, le degré de son échelle surpasse n.

La suite récurrente du premier degré est donnée par l'échelle

$$u - a \triangleq 0:$$

c'est une *progression géométrique* de raison a, et un terme quelconque a pour expression

$$u_n = A a^n:$$

Si l'échelle est

$$(u-1)^2 \triangleq u^2 - 2u + 1 \triangleq 0,$$

chaque terme est la moyenne arithmétique des deux termes qui le comprennent et la suite est une *progression arithmétique* de raison quelconque. En général, si $\varphi(x)$ désigne un polynôme de degré n et si le terme général d'une suite est

$$u_p = \varphi(p),$$

on a une suite récurrente ayant pour échelle le développement de

$$(u-1)^n \triangleq 0,$$

comme cela résulte immédiatement du calcul des différences (n° 76).

Les suites récurrentes ont été étudiées par Cassini, Moivre, Euler, Lagrange et par D. André [1]. Nous avons donné, dans les Chapitres qui précèdent, quelques exemples de suites récurrentes linéaires, dont les coefficients n'étaient pas constants. Mais, dans ce qui va suivre, nous supposerons les coefficients constants.

172. Propriétés des suites récurrentes. — 1° Si l'on multiplie tous les termes d'une suite récurrente par un même nombre, on obtient une suite récurrente de même échelle.

2° Si l'on renverse le sens du numérotage des termes d'une

---

[1] Cassini, *Histoire de l'Académie royale des Sciences*, p. 309. Paris, 1680. Moivre, *Miscellanea analytica*, p. 27. — Euler, *Introductio in Analysin*, t. I. — Lagrange, *Œuvres complètes*, t. I, III et V. — D. André, *Annales de l'École Normale supérieure*, 3e série, t. VII; Paris, 1878.

suite, on obtient une nouvelle suite dont l'échelle s'obtient en remplaçant dans la première u par u^{-1}.

3° Si l'on multiplie tous les termes d'une suite récurrente par les termes successifs d'une progression géométrique de raison λ, on obtient une suite récurrente de même degré dont l'échelle se déduit de la première en remplaçant u par $u:\lambda$. On peut simplifier le calcul des suites récurrentes en supposant que le premier ou le dernier coefficient de l'échelle est égal à l'unité.

4° Si l'on multiplie les termes correspondants $u_p, v_p, w_p, \ldots$ de plusieurs suites récurrentes de même échelle par des constantes A, B, C, ..., la somme

$$\mathrm{A}u_p + \mathrm{B}v_p + \mathrm{C}w_p + \ldots$$

forme une suite récurrente de même échelle. En particulier, toute fonction linéaire et homogène d'un nombre quelconque de termes d'une suite récurrente est une suite de même échelle.

5° Il résulte des deux propriétés précédentes que, si l'on multiplie le terme général u_p d'une suite récurrente par $\lambda^p \varphi(\lambda)$, en désignant par $\varphi(\lambda)$ un polynôme en λ de degré quelconque, on obtient une suite dont l'échelle se déduit de la première en remplaçant u par $u:\lambda$.

6° On peut multiplier, *et non diviser*, l'échelle de récurrence $f(u)$ par un polynôme quelconque $\psi(u)$. En effet, soit

$$\psi(u) = \mathrm{A}u^r + \mathrm{B}u^{r-1} + \mathrm{C}u^{r-2} + \ldots;$$

on a, pour toute valeur entière de p,

$$u^p f(u) \bumpeq 0$$

et, par suite,

$$\begin{aligned}
&\mathrm{A}u^{p+r} f(u) \bumpeq 0,\\
&\mathrm{B}u^{p+r-1} f(u) \bumpeq 0,\\
&\mathrm{C}u^{p+r-2} f(u) \bumpeq 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots;
\end{aligned}$$

en ajoutant les égalités précédentes, il vient

$$u^p \psi(u) f(u) \bumpeq 0.$$

Ainsi les différents termes de la suite de FIBONACCI, d'ordre

quelconque (n° 6), qui vérifient la relation

$$u^n \triangleq u^{n-1} + u^{n-2} + u^{n-3} + \ldots + u^0,$$

vérifient la relation suivante, obtenue en multipliant les deux membres de l'égalité symbolique précédente par $(u - 1)$

$$u^{n+1} \triangleq 2u^n - u^0;$$

en d'autres termes

$$u_{p+n+1} = 2u_{n+p} - u_p.$$

Plus généralement, décomposons l'échelle en deux parties, et supposons que l'on ait, de diverses manières,

$$\begin{aligned} f_1(u) &\triangleq \varphi_1(u), \\ f_2(u) &\triangleq \varphi_2(u), \\ f_3(u) &\triangleq \varphi_3(u), \\ &\ldots\ldots\ldots\ldots\ldots; \end{aligned}$$

mais de telle sorte qu'en faisant passer les termes du second membre dans le premier on retrouve $f(u)$; on aura, en désignant par Ψ un polynôme quelconque à plusieurs variables, l'identité

$$\Psi(f_1, f_2, f_3, \ldots) \triangleq \Psi(\varphi_1, \varphi_2, \varphi_3, \ldots).$$

On obtient ainsi des relations, en nombre indéfini, entre les termes d'une suite récurrente quelconque ([1]).

173. Fonctions récurrentes fondamentales. — Parmi les suites récurrentes d'échelle donnée $f(u)$, de degré n, il y a lieu de considérer plus particulièrement celles pour lesquelles les n valeurs initiales sont toutes nulles, à l'exception de l'une d'elles, supposée égale à 1; nous les appellerons les fonctions récurrentes fondamentales. Désignons par i l'un des nombres entiers

$$0, 1, 2, \ldots, (n-1),$$

par j un entier quelconque et par L_i^j le terme d'indice j de la fonction fondamentale pour laquelle on suppose

$$L_i^i = 1 \quad \text{et} \quad L_i^j = 0.$$

([1]) Voir nos *Recherches sur plusieurs ouvrages de* Léonard de Pise *et Sur diverses questions d'Arithmétique supérieure*; p. 33-42. — Rome, 1877.

pour toutes les valeurs de j, de 0 à $(n-1)$, à l'exception de i. Un terme quelconque u_j d'une suite récurrente de l'échelle donnée, dont les valeurs initiales sont

$$u_0, u_1, u_2, \ldots, u_{n-1},$$

s'exprime en fonction linéaire et homogène des n fonctions fondamentales d'indice j, par la formule

$$(1) \qquad u_j \triangleq u_0 L_0^j + u_1 L_1^j + u_2 L_2^j \ldots + u_{n-1} L_{n-1}^j,$$

analogue à la formule d'interpolation de LAGRANGE (n° 105). En effet, les conditions initiales se trouvent vérifiées d'après la définition même des fonctions fondamentales; de plus, u_j vérifie la loi de récurrence, puisque c'est une fonction linéaire et homogène de fonctions qui subissent la même loi.

On peut encore exprimer un terme u_j d'une suite récurrente quelconque du $n^{\text{ième}}$ ordre, en fonction linéaire et homogène de n termes consécutifs d'une seule fonction fondamentale et ainsi, par exemple, de la fonction L_{n-1}, que nous désignerons, pour simplifier, par U. Soit l'échelle de récurrence

$$f(u) \triangleq u^n - p_1 u^{n-1} + p_2 u^{n-2} - p_3 u^{n-3} + \ldots;$$

posons

$$\begin{aligned} f_0 &= u_0, \\ f_1 &= u_1 - p_1 u_0, \\ f_2 &= u_2 - p_1 u_1 + p_2 u_0, \\ f_3 &= u_3 - p_1 u_2 + p_2 u_1 - p_3 u_0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

de telle sorte que f_j s'annule pour $j \geqslant n$. On a la formule suivante, analogue à la formule d'interpolation de NEWTON (n° 108),

$$(2) \qquad u_j = f_0 U_{j+n-1} + f_1 U_{j+n-2} + f_2 U_{j+n-3} + \ldots + f_{n-1} U_j.$$

En effet, cette formule est vérifiée par les conditions initiales, ainsi qu'on le voit en remplaçant j par l'un des nombres de 0 à $(n-1)$, et en calculant les coefficients des valeurs initiales u_0, $u_1, \ldots, u_{n-1}$; de plus, elle est soumise à la loi de récurrence, comme fonction linéaire et homogène de suites assujetties à la même loi.

174. Théorème de Lagrange. — Lorsque l'échelle est le produit de n facteurs linéaires donnés et que l'on a

$$f(u) = (u-a)(u-b)(u-c)\ldots(u-l),$$

en désignant par $a, b, c, \ldots, l$ des quantités inégales deux à deux, on peut exprimer un terme quelconque u_j d'une suite récurrente en fonction linéaire des puissances de même exposant de $a, b, c, \ldots, l$, par la formule

$$(1) \qquad u_j = \mathrm{A}a^j + \mathrm{B}b^j + \mathrm{C}c^j + \ldots + \mathrm{L}l^j.$$

En effet, les coefficients A, B, C, ..., L se déterminent au moyen des n valeurs initiales et consécutives

$$u_0, u_1, u_2, \ldots, u_{n-1},$$

par n équations du premier degré obtenues en remplaçant j par $0, 1, 2, \ldots, (n-1)$, dans la formule (1). Le déterminant des inconnues n'est pas nul, puisqu'il est égal à la fonction alternée fondamentale de Vandermonde.

Mais nous ferons observer que la formule précédente, qui représente le théorème de Lagrange, est illusoire dans le cas général, puisque l'on ne connaît presque jamais la décomposition de l'échelle en facteurs linéaires, ou que lorsque cette décomposition est obtenue, les quantités $a, b, c, \ldots, l$ n'étant connues qu'avec une certaine approximation, on ne peut en déduire des résultats exacts. Il est donc préférable de se servir des deux formules du numéro précédent et d'étudier les diverses formes de développement que l'on peut donner à U_j lorsque j est donné avec les coefficients de l'échelle.

Dans le cas général où les facteurs linéaires de l'échelle sont tous distincts, on peut aussi exprimer une suite récurrente quelconque en valeur linéaire et homogène de n termes consécutifs de la suite

$$s_j = a^j + b^j + c^j + \ldots + l^j,$$

en posant

$$(2) \qquad u_j = \alpha s_j + \beta s_{j+1} + \gamma s_{j+2} + \ldots + \lambda s_{j+n-1}.$$

On détermine les coefficients $\alpha, \beta, \gamma, \ldots, \lambda$, au moyen des va-

leurs initiales $u_0, u_1, u_2, \ldots, u_{n-1}$, par des équations linéaires et homogènes dont le déterminant est égal au *discriminant* de $f(u)$, c'est-à-dire au carré de la fonction alternée fondamentale (n° 166, *Ex. I*).

175. Récurrence des fonctions alternées. — Considérons le déterminant du $n^{\text{ième}}$ ordre

$$Q = \begin{vmatrix} \varphi(a) & \varphi(b) & \varphi(c) & \ldots \\ \chi(a) & \chi(b) & \chi(c) & \ldots \\ \psi(a) & \psi(b) & \psi(c) & \ldots \\ . & . & . & . . \end{vmatrix},$$

dans lequel nous supposons que $\varphi, \chi, \psi, \ldots$ désignent des polynômes quelconques; le déterminant Q est une fonction alternée des n quantités $a, b, c, \ldots, l$. Désignons encore par

$$f(u) \triangleq (u-a)(u-b)(u-c)\ldots(u-l)$$

l'échelle de récurrence et par Q_j le déterminant obtenu en remplaçant les éléments d'une ligne quelconque de Q par $a^j, b^j, \ldots, l^j$. Lorsque j varie, le déterminant Q_j forme une suite récurrente de l'échelle donnée, puisque c'est une fonction linéaire et homogène des mêmes puissances des n quantités $a, b, c, \ldots, l$; il en est de même du quotient de Q_j par le déterminant de Vandermonde.

Cela posé, remplaçons le déterminant Q par le déterminant V de Vandermonde; désignons par les grandes lettres $A_i, B_i, C_i, \ldots$ les mineurs qui correspondent aux éléments $a^i, b^i, c^i, \ldots$ du déterminant V, et par V_i^j le quotient par V du déterminant obtenu en remplaçant, dans le déterminant V, les éléments $a^i, b^i, c^i, \ldots$ par $a^j, b^j, c^j, \ldots$; le développement du déterminant donne

$$V.V_i^j = A_i a^j + B_i b^j + C_i c^j + \ldots + L_i l^j.$$

Mais V_i^j s'annule pour toutes les valeurs de j, de 0 à $(n-1)$, à l'exception de $j = i$; dans ce dernier cas, V_i^i est égal à 1. Par suite, V_i^j est identique avec la fonction récurrente fondamentale L_i^j de rang $(i+1)$.

Par conséquent, toute fonction récurrente fondamentale est le quotient par le déterminant V de Vandermonde du déterminant

obtenu en remplaçant une ligne de V par a^j, b^j, c^j, ...; c'est une fonction symétrique de a, b, c, ...

En particulier, la fonction U_j, de rang n, est donnée par l'expression

$$V.U_j = V_a a^j + V_b b^j + V_c c^j + \ldots + V_l l^j,$$

dans laquelle V_a, V_b, V_c, ..., V_l sont les fonctions alternées de $(n-1)$ des quantités a, b, c, ..., l; pour $n=2$, on a

$$U_j = \frac{a^j - b^j}{a-b},$$

et pour $n=3$, on a

$$U_j = \frac{(b-c)a^j + (c-a)b^j + (a-b)c^j}{(b-a)(c-a)(c-b)},$$

176. Multiplication des suites récurrentes. — Considérons deux suites récurrentes y_n et z_n du second ordre, vérifiant respectivement les échelles

$$f(y) \triangleq y^2 - py + q \triangleq 0,$$
$$\varphi(z) \triangleq z^2 - p'z + q' \triangleq 0;$$

nous allons démontrer que le produit $y_n z_n$ forme une suite récurrente. En effet, supposons

$$f(y) = (y-a)(y-b),$$
$$\varphi(z) = (z-a')(z-b');$$

les nombres y_n et z_n vérifient les relations

$$y_n = A a^n + B b^n,$$
$$z_n = A' a'^n + B' b'^n;$$

on a donc

$$y_n z_n = AA'(aa')^n + BB'(bb')^n + AB'(ab')^n + A'B(a'b)^n.$$

Par conséquent, le produit $u_n = y_n z_n$ est soumis à la loi de récurrence

$$(u-aa')(u-bb')(u-ab')(u-a'b) \triangleq 0.$$

Ainsi $y_n z_n$ est une suite récurrente du quatrième ordre, dont

l'échelle peut s'écrire sous l'une des formes (¹)

$$q'^2 f\left(\frac{u}{a'}\right) f\left(\frac{u}{b'}\right) = 0,$$

$$q^2 \varphi\left(\frac{u}{a}\right) \varphi\left(\frac{u}{b}\right) = 0,$$

ou, par le développement,

$$u^4 - pp'u^3 + (p^2q' + p'^2q - 2qq')u^2 - pp'qq'u + q^2q'^2 = 0.$$

(¹) On obtient l'échelle des u en exprimant que les polynômes en x, du second degré,

$$f(xu) \quad \text{et} \quad u^2\varphi\left(\frac{x}{u}\right),$$

ont un facteur commun, et en remplaçant ensuite u^2 par u. En général, le problème de la multiplication des suites récurrentes d'ordre quelconque revient au problème de l'élimination.

CHAPITRE XVIII.

LES FONCTIONS NUMÉRIQUES DU SECOND ORDRE.

---

177. Définition des fonctions U_n et V_n. — Nous appelons *fonction numérique du second ordre* toute fonction y_n d'un nombre entier n, positif ou négatif, qui est déterminée par deux valeurs initiales y_0 et y_1, et par l'échelle de récurrence du second degré

$$u^2 = pu - q,$$

dans laquelle p et q désignent deux nombres entiers, positifs ou négatifs, dont le produit n'est pas nul.

La *fonction fondamentale* U_n est donnée par les conditions initiales

$$U_0 = 0, \qquad U_1 = 1,$$

et la *fonction primordiale* V_n est donnée par les conditions initiales

$$V_0 = 2, \qquad V_1 = p;$$

on a donc, par définition,

$$(1) \qquad \begin{cases} U_{n+2} = p\,U_{n+1} - q\,U_n, \\ V_{n+2} = p\,V_{n+1} - q\,V_n. \end{cases}$$

On voit tout de suite, par le calcul des U et des V pour les premières valeurs de n, que l'on a les relations

$$(2) \qquad U_{-n} = -\frac{U_n}{q^n}, \qquad V_{-n} = +\frac{V_n}{q^n}.$$

La fonction générale y_n s'exprime au moyen des valeurs initiales y_0 et y_1 et des fonctions U et V, par l'une des formules

$$(3) \qquad y_n = y_1\,U_n - q y_0\,U_{n-1},$$

$$(3') \qquad y_n = y_0\,U_{n+1} + (y_1 - p y_0)\,U_n.$$

En effet, ces formules sont vérifiées pour $n = 1$ et pour $n = 2$; on sait d'ailleurs que toute somme algébrique de fonctions numériques du même ordre, assujetties à une même loi de récurrence, est aussi une fonction numérique du même ordre assujettie à la même loi. En particulier, on a

$$(4) \qquad V_n = pU_n - 2qU_{n-1},$$

$$(4') \qquad V_n = 2U_{n+1} - pU_n.$$

Enfin, l'élimination de U_{n-1} entre deux des formules précédentes permet d'exprimer y_n en fonction linéaire de U_n et V_n par la formule

$$(5) \qquad 2y_n = (2y_1 - py_0)U_n + y_0V_n.$$

178. Les trois genres de fonctions numériques. — On classe les fonctions du second ordre d'après la nature du *discriminant*

$$\Delta = p^2 - 4q$$

de l'échelle de récurrence, écrite sous la forme

$$(2u - p)^2 = \Delta.$$

Si l'on suppose d'abord

$$p = 2a \quad \text{et} \quad q = a^2,$$

on trouve $\Delta = 0$, et

$$(1) \qquad U_n = na^{n-1}, \qquad V_n = a^n.$$

En particulier, pour

$$a = 1, \qquad p = 2, \qquad q = 1,$$

on a

$$U_n = n, \qquad V_n = 2,$$

et la fonction U_n représente la *suite naturelle des nombres entiers*. Cette remarque est importante, car dans toutes les formules de ce Chapitre les hypothèses particulières qui précèdent fourniront soit des vérifications, soit des formules plus simples.

Ainsi, pour $\Delta = 0$, la fonction générale y_n se réduit, soit à une *progression arithmétique,* soit à une *progression géométrique;*

d'ailleurs, on voit facilement que toute progression, arithmétique ou géométrique, peut être considérée comme une suite récurrente du second ordre.

En laissant de côté le cas singulier de $\Delta = 0$, on doit considérer trois cas différents, auxquels correspondent trois genres de fonctions numériques.

Premier genre. — Lorsque Δ est le carré d'un nombre entier δ, l'échelle se décompose en deux facteurs linéaires et l'on a

$$u^2 - pu + q = (u-a)(u-b),$$

en posant

$$a = \frac{p+\delta}{2}, \qquad b = \frac{p-\delta}{2}.$$

Alors U_n et V_n s'expriment par les formules

(2) $$U_n = \frac{a^n - b^n}{a-b}, \qquad V_n = a^n + b^n;$$

en effet, ces formules sont exactes pour les conditions initiales $n = 0$ et $n = 1$; d'ailleurs, a^n et b^n vérifient la loi de récurrence, puisque l'on a

$$p = a + b, \qquad q = ab;$$

il en est donc de même de leur somme et aussi de leur différence divisée par $\delta = (a-b)$.

On a encore la relation immédiate

(3) $$U_{2n} = U_n V_n,$$

qui s'applique aux fonctions des autres genres, ainsi que nous le démontrerons plus loin.

Parmi les fonctions du premier genre, nous considérerons plus spécialement les suites récurrentes données par les hypothèses

$$p = 3, \qquad q = 2,$$

pour lesquelles

$$\Delta = 1, \qquad a = 2, \qquad b = 1;$$

par conséquent,

$$U_n = 2^n - 1, \qquad V_n = 2^n + 1.$$

Les premières valeurs de ces fonctions, que nous désignerons sous le nom de *Suites de* FERMAT, sont renfermées dans le Tableau suivant :

Premier genre : $u^2 \triangleq 3u - 2$. $\Delta = 1$.

n	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
U_n	0,	1,	3,	7,	15,	31,	63,	127,	255,	511,	1023,
V_n	2,	3,	5,	9,	17,	33,	65,	129,	257,	513,	1025.

Suites de FERMAT.

Deuxième genre. — Lorsque Δ est un entier positif qui n'est pas le carré d'un nombre entier, l'échelle n'est plus décomposable en deux facteurs linéaires, et l'on obtient les fonctions du second genre. Il en est ainsi, par exemple, dans les hypothèses

$$p = 1, \qquad q = -1,$$

pour lesquelles $\Delta = 5$; on obtient alors les *Suites* de FIBONACCI [1] :

Deuxième genre : $u^2 \triangleq u + 1$. $\Delta = 5$.

n	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
U_n	0,	1,	1,	2,	3,	5,	8,	13,	21,	34,	55,
V_n	2,	1,	3,	4,	7,	11,	18,	29,	47,	76,	123.

Suites de FIBONACCI.

Nous prendrons encore pour exemple de fonctions du deuxième genre, les suites récurrentes définies par les hypothèses

$$p = 2, \qquad q = -1,$$

pour lesquelles $\Delta = 8$, et que nous appellerons *Suites de* PELL :

Deuxième genre : $u^2 \triangleq 2u + 1$. $\Delta = 8$.

n	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
U_n	0,	1,	2,	5,	12,	29,	70,	169,	408,	985,	2378,
V_n	2,	2,	6,	14,	34,	82,	198,	478,	1154,	2786,	6726.

Suites de PELL.

Troisième genre. — Lorsque Δ est un entier négatif, on obtient les fonctions du troisième genre. Les plus simples proviennent des hypothèses

$$p = 1, \qquad q = 1,$$

---

(1) *Scritti di Leonardo Pisano, matematico del secolo decimoterzo*, t. I, p. 283.

pour lesquelles $\Delta = -3$, et l'on trouve (n° 13),

$$\begin{cases} U_{3n} = 0, & U_{3n+1} = (-1)^n, & U_{3n+2} = (-1)^n, \\ V_{3n} = (-1)^n 2, & V_{3n+1} = (-1)^n, & V_{3n+2} = (-1)^{n+1}. \end{cases}$$

Nous considérerons encore les fonctions du troisième genre qui proviennent des hypothèses

$$p = 2, \qquad q = 3,$$

pour lesquelles $\Delta = -8$, et que nous appellerons *Suites conjuguées de* PELL :

Troisième genre : $u^2 \triangleq 2u - 3$. $\quad \Delta = -8$.

n	0,	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
U_n	0,	1,	2,	1,	−4,	−11,	−10,	13,	56,	73,	−22,
V_n	2,	2,	2,	−10,	−14,	2,	46,	86,	34,	−190,	−492.

Suites conjuguées de PELL.

Enfin, pour la vérification ou pour la simplification des formules de cette théorie, nous considérerons encore les fonctions du troisième genre données par les hypothèses

$$p = 2, \qquad q = 2,$$

pour lesquelles $\Delta = -4$. On a alors

$$\begin{cases} U_{4n} = 0, & U_{4n+1} = (-1)^n . 2^{2n}, & U_{4n+2} = U_{4n+3} = (-1)^n . 2^{2n+1}, \\ V_{4n} = V_{4n+1} = (-1)^n . 2^{2n+1}, & V_{4n+2} = 0, & V_{4n+3} = (-1)^n . 2^{2n}. \end{cases}$$

179. Développements de U_n et de V_n suivant les puissances de p et de q. — En calculant par l'échelle de récurrence les valeurs de U_n qui correspondent aux premiers nombres 1, 2, 3, 4, ..., on trouve

$$\begin{aligned}
U_1 &= 1, \\
U_2 &= p, \\
U_3 &= p^2 - q, \\
U_4 &= p^3 - 2pq, \\
U_5 &= p^4 - 3p^2q + q^2, \\
U_6 &= p^5 - 4p^3q + 3pq^2, \\
U_7 &= p^6 - 5p^4q + 6p^2q^2 - q^3, \\
U_8 &= p^7 - 6p^5q + 10p^3q^2 - 4pq^3, \\
U_9 &= p^8 - 7p^6q + 15p^4q^2 - 10p^2q^3 + q^4.
\end{aligned}$$

On voit ainsi que, pour les trois genres, la fonction U_n est un polynôme homogène de degré $(n-1)$ en p et q, en y considérant p au premier degré et q au second ; de plus, le premier coefficient est 1 et les autres coefficients sont alternativement positifs et négatifs ; d'ailleurs, le polynôme U_n ne contient que les puissances de p, dont l'exposant est de parité contraire à l'indice n de U_n.

Si l'on construit le Tableau à double entrée des coefficients pris en valeur absolue, en remontant d'une ligne ceux de la seconde colonne, de deux lignes ceux de la troisième colonne, et ainsi de suite, on obtient le triangle arithmétique de Pascal.

On a donc, par induction, la formule suivante, que l'on peut vérifier *a posteriori*,

$$(1)\qquad \left\{ \begin{aligned} U_{n+1} &= p^n - C_{n-1}^1 p^{n-2} q + C_{n-2}^2 p^{n-4} q^2 + \dots \\ &\quad + (-1)^r C_{n-r}^r p^{n-r} q^r + \dots . \end{aligned} \right.$$

Exemple I. — En particulier, pour $p = 1$ et $q = -1$, on retrouve la formule E (n° 13, *Ex. II*) ; pour $p = 1$ et $q = 1$, on retrouve la formule F.

Exemple II. — Pour $p = 2$ et $q = 1$ (suite naturelle des nombres entiers), on a

$$n + 1 = 2^n - C_{n-1}^1 2^{n-2} + C_{n-2}^2 2^{n-4} - \dots .$$

On peut aussi développer V_n suivant les puissances de p et de q, d'après la loi de formation. On trouve pour les premières valeurs de n

$$\begin{aligned}
V_0 &= 2, \\
V_1 &= p, \\
V_2 &= p^2 - 2q, \\
V_3 &= p^3 - 3pq, \\
V_4 &= p^4 - 4p^2 q + 2q^2, \\
V_5 &= p^5 - 5p^3 q + 5pq^2, \\
V_6 &= p^6 - 6p^4 q + 9p^2 q^2 - 2q^3, \\
V_7 &= p^7 - 7p^5 q + 14p^3 q^2 - 7pq^3, \\
V_8 &= p^8 - 8p^6 q + 20p^4 q^2 - 16p^2 q^3 + 2q^4, \\
V_9 &= p^9 - 9p^7 q + 27p^5 q^2 - 30p^3 q^3 + 9pq^4, \\
&\dots\dots\dots
\end{aligned}$$

Ainsi V_n est un polynôme homogène de degré n en p et q, en y considérant p au premier degré et q au second, qui ne contient que les puissances de p dont l'exposant est de même parité que

l'indice. On peut construire le tableau des coefficients pris en valeur absolue; en remontant d'une ligne les nombres de la seconde colonne, de deux lignes ceux de la troisième colonne, et ainsi de suite, on trouve que le tableau des coefficients forme alors un tableau de sommes, ainsi que cela résulte immédiatement de l'échelle de récurrence. On arrive plus rapidement au résultat par la formule (1) du n° 156, et l'on trouve ainsi

$$(2)\quad \left\{\begin{aligned} V_n &= p^n - \frac{n}{1} p^{n-2} q + \frac{n(n-3)}{1.2} p^{n-4} q^2 - \ldots \\ &\quad + (-1)^h \frac{n}{h} C_{n-h-1}^{h-1} p^{n-2h} q^h + \ldots, \end{aligned}\right.$$

car il suffit de calculer le coefficient de $p^{n-2h} q^h$.

180. Généralisation des formules. — Lorsqu'il s'agit de fonctions numériques du premier genre, nous avons vu (n° 178) que U_n et V_n s'expriment par les formules

$$U_n = \frac{a^n - b^n}{a - b}, \qquad V_n = a^n + b^n,$$

en fonction de deux nombres entiers a et b; on a d'ailleurs

$$p = a + b, \qquad q = ab, \qquad \delta = a - b.$$

Mais, au lieu des deux nombres entiers a et b qui définissent, dans ce cas, les fonctions U et V, on peut considérer les nombres a^r et b^r, en désignant par r un entier quelconque, positif ou négatif; on a alors, en désignant par des accents les fonctions correspondantes,

$$U'_n = \frac{a^{rn} - b^{rn}}{a^r - b^r}, \qquad V'_n = a^{rn} + b^{rn}$$

et

$$p' = a^r + b^r, \qquad q' = a^r b^r, \qquad \delta' = a^r - b^r.$$

D'autre part, si nous changeons n en rn dans les formules (1), nous obtenons

$$U_{rn} = \frac{a^{rn} - b^{rn}}{a - b}, \qquad V_{rn} = a^{rn} + b^{rn}.$$

On a donc

$$U'_n = \frac{U_{rn}}{U_r}, \qquad V'_n = V_{rn}.$$

mais les fonctions U'_n et V'_n vérifient les formules de récurrence

$$U'_{n+2} = p' U'_{n+1} - q' U'_n,$$
$$V'_{n+2} = p' V'_{n+1} - q' V'_n;$$

et l'on a

$$p' = V_r, \qquad q' = q^r, \qquad \Delta' = \Delta U_r^2.$$

Par conséquent, pour les fonctions numériques du premier genre, *on généralise toutes les formules qui contiennent* U_n *et* V_n, *en y remplaçant*

$$U_n \textit{ par } \frac{U_{nr}}{U_r}, \qquad V_n \textit{ par } V_{nr},$$

et

$$p \textit{ par } V_r, \qquad q \textit{ par } q^r, \qquad \Delta \textit{ par } \Delta U_r^2.$$

Il semble que cette généralisation ne peut s'appliquer qu'aux fonctions du premier genre; mais nous devons observer que si les formules obtenues ne contiennent ni a, ni b, ni δ, mais seulement les fonctions U et V et les nombres p, q, Δ, on peut étendre aux fonctions du second genre, et du troisième, le procédé de généralisation que nous venons d'indiquer. En effet, lorsque l'on remplace U_n et V_n par des polynômes homogènes en p et q, ou par des polynômes homogènes en p et Δ (p étant au premier degré, q et Δ au second degré), les formules donnent des identités, entre des polynômes de degré fini, qui sont vérifiées pour des systèmes de valeurs de p et de q, ou de p et Δ, en nombre aussi grand qu'on veut. Par conséquent, ces formules sont exactes, quelles que soient les valeurs de p, q, Δ. Ainsi, en résumé, *toute formule démontrée pour les fonctions numériques du premier genre s'applique aux fonctions numériques des autres genres, lorsque cette formule ne contient ni* a, *ni* b, *ni* δ, *mais seulement les nombres* p, q, Δ.

181. Formules d'addition des arguments. — En résolvant par rapport à a^n et b^n les deux formules

$$a^n - b^n = \delta U_n, \qquad a^n + b^n = V^n,$$

on trouve immédiatement

$$(1) \qquad 2a^n = V_n + \delta U_n, \qquad 2b^n = V_n - \delta U_n.$$

Cela posé, considérons deux valeurs m et n de l'indice, nous aurons

$$2a^m = V_m + \delta U_m, \qquad 2a^n = V_n + \delta U_n;$$

multiplions membre à membre les deux formules, nous obtenons

$$4a^{m+n} = V_m V_n + \Delta U_m U_n + \delta(U_m V_n + U_n V_m).$$

Si nous changeons a en b et δ en $-\delta$, nous obtenons une autre formule; puis, par addition et par soustraction,

$$(2) \qquad \begin{cases} 2U_{m+n} = U_m V_n + U_n V_m, \\ 2V_{m+n} = V_m V_n + \Delta U_m U_n. \end{cases}$$

Ces formules permettent de calculer les valeurs de U et de V qui correspondent à l'indice ou argument $(m+n)$, lorsque l'on connaît les valeurs de U et de V pour les arguments m et n; en changeant n en $-n$, on trouve encore, en tenant compte des formules (2) du n° 177,

$$(3) \qquad \begin{cases} 2q^n U_{m-n} = U_m V_n - U_n V_m, \\ 2q^n V_{m-n} = V_m V_n - \Delta U_m U_n. \end{cases}$$

Ces dernières relations permettent de calculer les valeurs de U et de V pour l'argument $(m-n)$. Plus généralement, on peut obtenir des formules pour calculer les valeurs de U et de V qui correspondent à l'argument $(n_1 + n_2 + n_3 + \ldots)$, lorsque l'on connaît les valeurs de ces fonctions pour les arguments n_1, n_2, n_3, ..., positifs ou négatifs.

La première des formules (2) peut s'écrire

$$2\,\frac{U_{m+n}}{U_n} = \frac{U_m}{U_n} V_n + V_m;$$

on a donc

$$2\,\frac{U_{m+n} U_{m+n-1} \ldots U_{m+1}}{U_n U_{n-1} \ldots U_1} = \frac{U_{m+n-1} U_{m+n-2} \ldots U_m}{U_n U_{n-1} \ldots U_1} V_n + \frac{U_{m+n-1} \ldots U_{m+1}}{U_{n-1} \ldots U_1} V_m;$$

par conséquent, en ne tenant pas compte du facteur 2, on a ce théorème :

Le produit de n termes consécutifs de la série U_n, *pour des*

indices positifs, est divisible par le produit des n premiers termes $U_1, U_2, \ldots, U_n$.

182. Développements de U_n et de V_n suivant les puissances de p et de Δ. — On a les formules

$$2a = p + \delta,$$
$$2b = p - \delta;$$

par conséquent, en élevant les deux membres à la puissance d'exposant n, il vient

$$2^n a^n = p^n + C_n^1 p^{n-1}\delta + C_n^2 p^{n-2}\delta^2 + C_n^3 p^{n-3}\delta^3 + \ldots,$$
$$2^n b^n = p^n - C_n^1 p^{n-1}\delta + C_n^2 p^{n-2}\delta^2 - C_n^3 p^{n-3}\delta^3 + \ldots;$$

puis, par soustraction et par addition,

$$(1)\qquad \begin{cases} 2^{n-1} U_n = C_n^1 p^{n-1} + C_n^3 p^{n-3}\Delta + C_n^5 p^{n-5}\Delta^2 + \ldots, \\ 2^{n-1} V_n = \quad p^n \quad + C_n^2 p^{n-2}\Delta + C_n^4 p^{n-4}\Delta^2 + \ldots. \end{cases}$$

On peut encore se proposer de développer U_n et V_n suivant les puissances de Δ et de q; mais on obtient les formules correspondantes par le changement du signe de b et de q, et par l'échange de p^2 et Δ, en considérant les deux cas suivants :

1° Lorsque n est pair, toute formule contenant les nombres U_n, V_n se transforme en une autre, à la condition de conserver V_n et de remplacer U_n^2 par $\frac{\Delta U_n^2}{p^2}$.

2° Lorsque n est impair, on remplace V_n^2 par ΔU_n^2 et U_n par $(V_n : p)$.

183. Multiplication des arguments. — Si l'on suppose $m = n$, les formules d'addition des arguments donnent

$$\begin{cases} U_{2n} = U_n V_n, \\ 2V_{2n} = V_n^2 + \Delta U_n^2. \end{cases}$$

D'autre part, en multipliant membre à membre les formules (1) du n° 181, on obtient

$$(2)\qquad 4q^n = V_n^2 - \Delta U_n^2.$$

On déduit des formules (1) et (2)

$$(3)\qquad \begin{cases} V_{2n} = V_n^2 - 2q^n, \\ V_{2n} = \Delta U_n^2 + 2q^n. \end{cases}$$

Les formules précédentes permettent de calculer rapidement les valeurs de U_n et de V_n pour des valeurs de l'indice qui correspondent aux termes d'une progression géométrique de raison 2. Ce sont les formules de *duplication des arguments*.

On trouve encore, pour la *triplication des arguments*, les formules

$$(4)\qquad \begin{cases} \dfrac{U_{3n}}{U_n} = \Delta U_n^2 + 3q^n, & \dfrac{U_{3n}}{U_n} = V_n^2 - q^n, \\ \dfrac{V_{3n}}{V_n} = \Delta U_n^2 + q^n, & \dfrac{V_{3n}}{V_n} = V_n^2 - 3q^n. \end{cases}$$

Plus généralement, si nous appliquons le procédé exposé au n° 180, pour la généralisation des formules, aux développements de U_n et de V_n, suivant les puissances de p et de q (n° 179), nous obtenons

$$\begin{aligned} U_{2r} &= U_r V_r, \\ U_{3r} &= U_r[V_r^2 - q^r], \\ U_{4r} &= U_r[V_r^3 - 2q^r V_r], \\ U_{5r} &= U_r[V_r^4 - 3q^r V_r^2 + q^{2r}], \\ &\dots\dots\dots\dots\dots\dots \end{aligned}$$

et, en général,

$$\frac{U_{nr}}{U_r} = V_r^{n-1} - C_{n-2}^1 q^r V_r^{n-3} + C_{n-3}^2 q^{2r} V_r^{n-5} - \dots.$$

De même, on a encore

$$\begin{aligned} V_{2r} &= V_r^2 - 2q^r, \\ V_{3r} &= V_r^3 - 3q^r V^r, \\ V_{4r} &= V_r^4 - 4q^r V_r^2 + 2q^{2r}, \\ V_{5r} &= V_r^5 - 5q^r V_r^3 + 5q^{2r} V_r, \\ V_{6r} &= V_r^6 - 6q^r V_r^4 + 9q^{2r} V_r^2 - 2q^{3r}, \end{aligned}$$

et, en général,

$$\begin{aligned} V_{nr} = V_r^n - \frac{n}{1} q^r V_r^{n-2} + \frac{n(n-3)}{1.2} q^{2r} V_r^{n-4} - \dots \\ + (-1)^h \frac{n}{h} C_{p-h-1}^{h-1} q^{hr} V_r^{n-2h} + \dots. \end{aligned}$$

Les développements de U_n et de V_n suivant les puissances de p et de Δ donnent, de même

$$2^{n-1}\frac{U_{nr}}{U_r} = C_n^1 V_r^{n-1} + C_n^3 \Delta U_r^2 V_r^{n-3} + C_n^5 \Delta^2 U_r^4 V_r^{n-5} + \ldots,$$
$$2^{n-1} V_{nr} = \quad V_r^n \quad + C_n^2 \Delta U_r^2 V_r^{n-2} + C_n^4 \Delta^2 U_r^4 V_r^{n-4} + \ldots.$$

184. Fonctions circulaires et fonctions hyperboliques. — La théorie des fonctions numériques du second ordre permet de simplifier considérablement la théorie des fonctions circulaires et des fonctions hyperboliques.

Après avoir défini les *fonctions circulaires* et démontré les formules d'addition des arcs, on arrive aux formules de Simpson

$$\sin(n+2)x = 2\cos x \sin(n+1)x - \sin nx,$$
$$\cos(n+2)x = 2\cos x \cos(n+1)x - \cos nx.$$

Par conséquent, si l'on pose

$$(1) \qquad \begin{cases} U_n = \dfrac{\sin nx}{\sin x}, & V_n = 2\cos nx, \\ p = 2\cos x, \quad q = +1, & \Delta = -4\sin^2 x, \end{cases}$$

on voit que U_n et V_n vérifient l'échelle de récurrence

$$u^2 \triangleq pu - q;$$

d'ailleurs, U_n prend les valeurs 0 et 1 pour $n = 0$ et $n = 1$, tandis que V_n prend les valeurs 2 et p; par conséquent, *à toute formule de la théorie des fonctions numériques du second ordre correspond une formule de la théorie des fonctions circulaires, au moyen des formules de transformation* (1) *ci-dessus.*

Puisque Δ est négatif, les fonctions circulaires peuvent être considérées comme des fonctions du troisième genre.

Ainsi aux formules (2) du n° **181** correspondent les formules d'addition des arcs; aux formules (1) du n° **182** correspondent les formules pour le développement de $(\sin nx : \sin x)$ et de $\cos nx$ suivant les puissances du cosinus et du sinus de l'arc x; ces formules ont été données par Jean Bernoulli, dans les *Acta Lipsiæ* (1701). La transformation de la formule (1) du n° **179** conduit au développement de $(\sin nx : \sin x)$ suivant les puissances de $\cos x$, formule

On déduit des formules (1) et (2)

$$(3)\qquad \begin{cases} V_{2n} = V_n^2 - 2q^n, \\ V_{2n} = \Delta U_n^2 + 2q^n. \end{cases}$$

Les formules précédentes permettent de calculer rapidement les valeurs de U_n et de V_n pour des valeurs de l'indice qui correspondent aux termes d'une progression géométrique de raison 2. Ce sont les formules de *duplication des arguments*.

On trouve encore, pour la *triplication des arguments*, les formules

$$(4)\qquad \begin{cases} \dfrac{U_{3n}}{U_n} = \Delta U_n^2 + 3q^n, & \dfrac{U_{3n}}{U_n} = V_n^2 - q^n, \\ \dfrac{V_{3n}}{V_n} = \Delta U_n^2 + q^n, & \dfrac{V_{3n}}{V_n} = V_n^2 - 3q^n. \end{cases}$$

Plus généralement, si nous appliquons le procédé exposé au n° 180, pour la généralisation des formules, aux développements de U_n et de V_n, suivant les puissances de p et de q (n° 179), nous obtenons

$$\begin{aligned} U_{2r} &= U_r V_r, \\ U_{3r} &= U_r[V_r^2 - q^r], \\ U_{4r} &= U_r[V_r^3 - 2q^r V_r], \\ U_{5r} &= U_r[V_r^4 - 3q^r V_r^2 + q^{2r}], \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

et, en général,

$$\frac{U_{nr}}{U_r} = V_r^{n-1} - C_{n-2}^1 q^r V_r^{n-3} + C_{n-3}^2 q^{2r} V_r^{n-5} - \ldots.$$

De même, on a encore

$$\begin{aligned} V_{2r} &= V_r^2 - 2q^r, \\ V_{3r} &= V_r^3 - 3q^r V_r, \\ V_{4r} &= V_r^4 - 4q^r V_r^2 + 2q^{2r}, \\ V_{5r} &= V_r^5 - 5q^r V_r^3 + 5q^{2r} V_r, \\ V_{6r} &= V_r^6 - 6q^r V_r^4 + 9q^{2r} V_r^2 - 2q^{3r}, \end{aligned}$$

et, en général,

$$\begin{aligned} V_{nr} = V_r^n - \frac{n}{1} q^r V_r^{n-2} + \frac{n(n-3)}{1\cdot 2} q^{2r} V_r^{n-4} - \ldots \\ \pm \frac{n}{k} C_{n-k-1}^{k-1} q^{kr} V_r^{n-2k} \pm \ldots. \end{aligned}$$

Les développements de U_n et de V_n suivant les puissances de p et de Δ donnent, de même

$$2^{n-1}\frac{U_{nr}}{U_r} = C_n^1 V_r^{n-1} + C_n^3 \Delta U_r^2 V_r^{n-3} + C_n^5 \Delta^2 U_r^4 V_r^{n-5} + \ldots,$$
$$2^{n-1} V_{nr} = V_r^n + C_n^2 \Delta U_r^2 V_r^{n-2} + C_n^4 \Delta^2 U_r^4 V_r^{n-4} + \ldots.$$

184. Fonctions circulaires et fonctions hyperboliques. — La théorie des fonctions numériques du second ordre permet de simplifier considérablement la théorie des fonctions circulaires et des fonctions hyperboliques.

Après avoir défini les *fonctions circulaires* et démontré les formules d'addition des arcs, on arrive aux formules de SIMPSON

$$\sin(n+2)x = 2\cos x \sin(n+1)x - \sin nx,$$
$$\cos(n+2)x = 2\cos x \cos(n+1)x - \cos nx.$$

Par conséquent, si l'on pose

$$(1)\qquad \begin{cases} U_n = \dfrac{\sin nx}{\sin x}, & V_n = 2\cos nx, \\ p = 2\cos x, \quad q = +1, & \Delta = -4\sin^2 x, \end{cases}$$

on voit que U_n et V_n vérifient l'échelle de récurrence

$$u^2 \triangleq pu - q;$$

d'ailleurs, U_n prend les valeurs 0 et 1 pour $n = 0$ et $n = 1$, tandis que V_n prend les valeurs 2 et p; par conséquent, *à toute formule de la théorie des fonctions numériques du second ordre correspond une formule de la théorie des fonctions circulaires, au moyen des formules de transformation* (1) *ci-dessus*.

Puisque Δ est négatif, les fonctions circulaires peuvent être considérées comme des fonctions du troisième genre.

Ainsi aux formules (2) du n° **181** correspondent les formules d'addition des arcs; aux formules (1) du n° **182** correspondent les formules pour le développement de $(\sin nx : \sin x)$ et de $\cos nx$ suivant les puissances du cosinus et du sinus de l'arc x; ces formules ont été données par JEAN BERNOULLI, dans les *Acta Lipsiæ* (1701). La transformation de la formule (1) du n° **179** conduit au développement de $(\sin nx : \sin x)$ suivant les puissances de $\cos x$, formule

donnée par Viète (*Opera*, p. 296-299. — Leyde 1646). La transformation de la formule (2) du n° 179 conduit au développement de $\cos nx$ suivant les puissances de $\cos x$, formule donnée par Moivre (*Commentarii Acad. Petrop.*, t. XIII, p. 29; 1741).

De même, après avoir défini les *fonctions hyperboliques*, on arrive à des formules analogues à celles de Simpson. Par conséquent, si l'on pose

$$(2)\qquad \begin{cases} U_n = \dfrac{\sin\text{hyp}\, nx}{\sin\text{hyp}\, x}, & V_n = 2\cos\text{hyp}\, nx, \\ p = 2\cos\text{hyp}\, x, \quad q = +1, & \Delta = +4\sin\text{hyp}^2 x, \end{cases}$$

il en résulte, comme ci-dessus, la proposition suivante : *A toute formule de la théorie des fonctions numériques du second ordre correspond une formule de la théorie des fonctions hyperboliques, au moyen des formules* (2) *de transformation.* Puisque Δ est positif, les fonctions hyperboliques peuvent être considérées comme des fonctions numériques du second genre.

On voit ainsi que toutes les formules de la Trigonométrie du cercle et de l'hyperbole équilatère peuvent s'établir sans avoir recours aux imaginaires et à la formule de Moivre. Cependant, si l'on veut établir la correspondance entre les fonctions trigonométriques et les fonctions numériques du second ordre, il est facile de montrer que l'on a, en partant de la formule d'Euler

$$\cos x + i\sin x = e^{xi},$$

les relations

$$V_{2x} = 2q^x \cos\left(ni \operatorname{Log}\frac{a}{b}\right),$$

$$\sqrt{-\Delta}\, U_{2x} = 2q^x \sin\left(ni \operatorname{Log}\frac{a}{b}\right).$$

185. Développements des puissances de U_x et de V_x, en somme algébrique de fonctions dont les arguments sont des multiples de n. — En groupant les termes équidistants des extrêmes, la formule du binôme peut s'écrire

$$(z+\zeta)^n = z^n + \zeta^n + C_n^1 z\zeta(z^{n-2} + \zeta^{n-2}) + C_n^2 z^2\zeta^2(z^{n-4} + \zeta^{n-4}) + \ldots;$$

par conséquent, si l'on suppose $z = a^x$ et $\zeta = b^x$, on a, en supposant $n = 2\nu$, le développement

$$(1)\qquad V_x^n = V_{nx} + C_n^1 q^x V_{(n-2)x} + C_n^2 q^{2x} V_{(n-4)x} + \ldots + C_n^\nu q^{\nu x}.$$

et en supposant $r = 2\rho + 1$,

$$(1') \qquad V_n^r = V_{rn} + C_r^1 q^n V_{(r-2)n} + C_r^2 q^{2n} V_{(r-4)n} + \ldots + C_r^\rho q^{\rho n} V_n.$$

Ainsi, pour les premières valeurs de r, on forme le tableau

$$\begin{aligned}
V_n^2 &= V_{2n} + 2q^n,\\
V_n^3 &= V_{3n} + 3q^n V_n,\\
V_n^4 &= V_{4n} + 4q^n V_{2n} + 6q^{2n},\\
V_n^5 &= V_{5n} + 5q^n V_{3n} + 10q^{2n} V_n,\\
V_n^6 &= V_{6n} + 6q^n V_{4n} + 15q^{2n} V_{2n} + 20q^{3n},\\
V_n^7 &= V_{7n} + 7q^n V_{5n} + 21q^{2n} V_{3n} + 35q^{3n} V_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

De même, le développement de $(\alpha - \beta)^r$ donne, en supposant $r = 2\rho$,

$$(2) \quad \Delta^\rho U_n^r = V_{rn} - C_r^1 q^n V_{(r-2)n} + C_r^2 q^{2n} V_{(r-4)n} - \ldots + (-1)^\rho C_r^\rho q^{\rho n};$$

et en supposant $r = 2\rho + 1$,

$$(2') \quad \Delta^\rho U_n^r = U_{rn} - C_r^1 q^n U_{(r-2)n} + C_r^2 q^{2n} U_{(r-4)n} - \ldots + (-1)^\rho C_r^\rho q^{\rho n} U_n.$$

Ainsi, pour les premières valeurs paires de r, on a

$$\begin{aligned}
\Delta\, U_n^2 &= V_{2n} - 2q^n,\\
\Delta^2 U_n^4 &= V_{4n} - 4q^n V_{2n} + 6q^{2n},\\
\Delta^3 U_n^6 &= V_{6n} - 6q^n V_{4n} + 15q^{2n} V_{2n} - 20q^{3n},\\
\Delta^4 U_n^8 &= V_{8n} - 8q^n V_{6n} + 28q^{2n} V_{4n} - 56q^{3n} V_{2n} + 70q^{4n},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;
\end{aligned}$$

et pour les premières valeurs impaires de r,

$$\begin{aligned}
\Delta\, U_n^3 &= U_{3n} - 3q^n U_n,\\
\Delta^2 U_n^5 &= U_{5n} - 5q^n U_{3n} + 10q^{2n} U_n,\\
\Delta^3 U_n^7 &= U_{7n} - 7q^n U_{5n} + 21q^{2n} U_{3n} - 35q^{3n} U_n,\\
\Delta^4 U_n^9 &= U_{9n} - 9q_n U_{7n} + 36q^{2n} U_{5n} - 84q^{3n} U_{3n} + 126q^{4n} U_n,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Le développement de la puissance d'un binôme donne encore d'autres formules ; ainsi l'on a

$$\alpha = \overline{\alpha + \beta} - \beta, \qquad \text{et} \qquad \beta = \overline{\alpha + \beta} - \alpha;$$

donc en élevant les deux membres à une puissance d'exposant *impair r*, il vient

$$\alpha^r + \beta^r = (\alpha - \beta)^r - C_r^1 \beta(\alpha - \beta)^{r-1} - \ldots - C_r^1 \beta^{r-1}(\alpha - \beta)$$

et

$$\beta^r + \alpha^r = (\alpha + \beta)^r - C_r^1 \alpha(\alpha + \beta)^{r-1} - \ldots + C_r^1 \alpha^{r-1}(\alpha + \beta);$$

par suite, par addition et par soustraction, après avoir remplacé α par a^n et β par b^n, en tenant compte des formules (1) du n° **180**,

$$\begin{aligned} 2V_{rn} &= V_0 V_n^r - C_r^1 V_n V_n^{r-1} - C_r^2 V_{2n} V_n^{r-2} - \ldots + C_r^1 V_{(r-1)n} V_n, \\ 0 &= \phantom{V_0 V_n^r - {}} C_r^1 U_n V_n^{r-1} - C_r^2 U_{2n} V_n^{r-2} - \ldots + C_r^1 U_{(r-1)n} V_n. \end{aligned}$$

On obtient deux autres formules en supposant r pair. De plus, le développement des puissances de

$$\alpha = \overline{\alpha - \beta} + \beta, \qquad \text{et} \qquad \beta = \overline{\beta - \alpha} - \alpha$$

donne encore deux autres formules.

186. Sommation des fonctions U et V. — Nous avons trouvé, pour l'addition des arguments (n° **181**), les formules

$$\begin{aligned} 2U_{m+n} &= U_m V_n + U_n V_m, \\ 2V_{m+n} &= V_m V_n + \Delta\, U_m U_n; \end{aligned}$$

et pour la soustraction, les formules

$$\begin{aligned} 2q^n U_{m-n} &= U_m V_n - U_n V_m, \\ 2q^n V_{m-n} &= V_m V_n - \Delta\, U_m U_n. \end{aligned}$$

Si l'on pose

$$m + n = 2r, \qquad m - n = 2s,$$

dans les formules précédentes, on trouve ensuite, en les ajoutant ou en les soustrayant,

$$(1) \qquad \begin{cases} U_{2r} + q^{r-s} U_{2s} = U_{r+s} V_{r-s}, \\ U_{2r} - q^{r-s} U_{2s} = U_{r-s} V_{r+s}; \\ V_{2r} + q^{r-s} V_{2s} = V_{r+s} V_{r-s}, \\ V_{2r} - q^{r-s} V_{2s} = \Delta U_{r+s} U_{r-s}. \end{cases}$$

On déduit facilement de ces formules,

$$U_m + q^{-r}U_{m+2r} + q^{-2r}U_{m+4r} + \ldots + q^{-nr}U_{m+2nr} = q^{m-nr}\frac{U_{(n+1)r}}{U_r}U_{m+nr},$$

$$V_m + q^{-r}V_{m+2r} + q^{-2r}V_{m+4r} + \ldots + q^{-nr}V_{m+2nr} = q^{m-nr}\frac{U_{(n+1)r}}{U_r}V_{m+nr};$$

mais on trouve des formules plus générales par le procédé suivant.

Désignons par $a, b, c, \ldots, h, k, l$ les n termes d'une progression arithmétique de raison r; on a l'identité

$$V_c = V_r V_b - q^r V_a, \qquad U_c = V_r U_b - q^r U_a;$$

par suite, en remplaçant dans la première a, b, c par b, c, d, et ainsi de suite, il vient, en désignant encore par λ et μ les deux termes suivants de la progression arithmétique

$$\begin{aligned} U_c &= V_r U_b - q^r U_a, \\ U_d &= V_r U_c - q^r U_b, \\ U_e &= V_r U_d - q^r U_c, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ U_\mu &= V_r U_\lambda - q^r U_l. \end{aligned}$$

Multiplions respectivement ces égalités par $1, z, z^2, \ldots, z^{n-1}$, et ajoutons les résultats obtenus; en posant

$$\Sigma = U_a + zU_b + z^2U_c + \ldots + z^{n-1}U_l,$$

il vient

$$\frac{\Sigma - U_a - zU_b}{z^2} + z^{n-1}U_\mu + z^{n-2}U_\lambda = V_r\left(\frac{\Sigma - U_a}{z} + z^{n-1}U_\lambda\right) - q^r\Sigma,$$

d'où l'on tire

$$\Sigma = \frac{zU_b + (zV_r - 1)(z^nU_\lambda - U_a) - z^{n+1}U_\mu}{1 - zV_r + z^2q^r}.$$

Nous avons ainsi obtenu la somme des produits des fonctions U dont les arguments sont en progression arithmétique, multipliées respectivement par les termes d'une progression géométrique.

On obtient une formule analogue en remplaçant U par V dans le numérateur de Σ.

[illegible] **Décomposition des fonctions numériques.** — Considérons la formule de [illegible] des arguments

$$[illegible]$$

supposons [illegible]

$$[illegible]$$

par suite

$$[illegible]$$

Il en résulte cette proposition : *Lorsque dans l'échelle de [illegible]*

$$[illegible]$$

[illegible] la fonction numérique V_n [illegible] d'un nombre impair, est décomposable en un produit de deux facteurs [illegible].

En particulier, dans la suite de Fermat, on a

$$[illegible]$$

Cette formule a été indiquée pour la première fois par AURIFEUILLE, ancien élève de l'École Polytechnique, ancien professeur au lycée de Toulouse, qui nous l'a transmise par M. Le Lasseur.

Par exemple, pour $n = [illegible]$,

$$[illegible]$$

Cette décomposition, pour le cas de [illegible], a été obtenue antérieurement par M. F. Landry, au moyen d'une méthode inédite pour la recherche des diviseurs des grands nombres. Dans l'opuscule intitulé *Décomposition des nombres [illegible] en leurs facteurs premiers, de $n = 1$ à $n = 64$, moins quatre*, par M. F. Landry (Paris, [illegible]), l'auteur écrit à ce sujet : « De toutes les décompositions que nous avons opérées, aucune ne nous a demandé autant de temps et de patience que celle du nombre [illegible]. Les deux derniers facteurs de ce nombre ont neuf chiffres l'un et l'autre. Leur produit, qu'il s'agissait de décomposer, est le nombre de dix-sept chiffres

$$[illegible]$$

Si ces facteurs venaient à se perdre, le courage nous manquerait pour recommencer le travail, et il est probable que bien des âges passeraient avant qu'on ne réussît à les découvrir de nouveau. »

Ainsi la formule d'Aurifeuille avait échappé à l'attention d'Euler, de Lagrange, de Legendre, de Sophie Germain et de Landry, qui se sont occupés longuement et à diverses reprises de la décomposition en facteurs premiers des termes de la suite de Fermat. (Voir n° 34, *Exemple I.*)

Soit la formule

$$2V_{2n} = V_n^2 + \Delta U_n^2;$$

lorsque Δ est égal, en signe contraire, au carré d'un nombre entier, l'expression $2V_{2n}$ est une différence de deux carrés. Par suite : *Lorsque Δ est égal au carré d'un nombre entier, pris avec le signe —, la fonction V_{2n} est décomposable en un produit de deux facteurs entiers.*

Considérons encore la formule

$$V_{2n} = \Delta U_n^2 + 2q^n;$$

si l'on désigne ± 1 par ε et si l'on suppose

$$\Delta = 2\varepsilon h^2, \qquad q = -\varepsilon g^2, \qquad n = 2\mu + 1,$$

il vient

$$V_{2n} = 2\varepsilon(g^{2\mu+1} + hU_{2\mu+1})(g^{2\mu+1} - hU_{2\mu+1}).$$

On trouve un résultat analogue en supposant

$$\Delta = \varepsilon h^2, \qquad q = -\varepsilon g^2, \qquad n = 2\mu + 1;$$

par conséquent, on a la proposition suivante : *Lorsque le produit $q\Delta$ est égal et de signe contraire au double du carré d'un nombre entier, la fonction $V_{4\mu+2}$ est décomposable en un produit de deux facteurs entiers.*

Ainsi, par exemple, dans la suite de Pell,

$$V_{4\mu+2} = 2(2U_{\mu+1} + 1)(2U_{\mu+1} - 1).$$

Enfin, si nous supposons

$$\Delta = -2h^2 \qquad \text{et} \qquad n = 2\mu,$$

la même formule nous donne

$$V_{4\mu} = 2[q^n + hV_{2\mu}][q^n - hV_{2\mu}];$$

par conséquent : *lorsque Δ est égal et de signe contraire au*

double du carré d'un nombre entier, la fonction V_{4n} est décomposable en un produit de deux facteurs entiers.

Exemple I. — Donner les formules de décomposition de V_{2n} dans les hypothèses suivantes :

I......	$p = 2(r^2 - 2rs - s^2)$,	$q = -(r^2 - 2rs - s^2)^2$;
II.....	$p = 2(r^2 - 2s^2)$,	$q = (r^2 - 2s^2)^2$;
III.....	$p = r^2 - 2s^2$,	$q = -8r^2s^2$;
IV.....	$p = 2r$,	$q = r^2 - s^2$.

Voir, pour plus de renseignements, notre Mémoire *Sur la théorie des fonctions numériques simplement périodiques*, dans la *Nouv. Corresp. math.*, t. IV, p. 100.

En partant des formules pour la triplication des arguments (n° **183**), on arrive encore à la décomposition des fonctions numériques dans les cas suivants :

Le nombre $\frac{U_{3n}}{U_n}$ est décomposable en un produit de deux facteurs entiers, pour n pair, lorsque Δ est égal, en signe contraire, au triple du carré d'un nombre entier. Pour n impair, lorsque $q\Delta$ est égal, en signe contraire, au triple du carré d'un nombre entier.

Le nombre $\frac{V_{3n}}{V_n}$ est décomposable en un produit de deux facteurs entiers, pour n pair, lorsque Δ est égal et de signe contraire au carré d'un nombre entier. Pour n impair, lorsque q est le triple d'un carré entier, ou encore lorsque $q\Delta$ est égal et de signe contraire au triple du carré d'un nombre entier.

188. Sommation de fractions. — On a l'identité

$$\frac{U_{n+1}}{U_n} = \frac{U_2}{U_1} + \left(\frac{U_3}{U_2} - \frac{U_2}{U_1}\right) + \left(\frac{U_4}{U_3} - \frac{U_3}{U_2}\right) + \ldots + \left(\frac{U_{n+1}}{U_n} - \frac{U_n}{U_{n-1}}\right);$$

puis, en réunissant les fractions contenues dans chaque parenthèse,

$$\frac{U_{n+1}}{U_n} = \frac{U_2}{U_1} - \frac{q}{U_1U_2} - \frac{q^2}{U_2U_3} - \frac{q^3}{U_3U_4} - \ldots - \frac{q^{n-1}}{U_{n-1}U_n}.$$

On a, par exemple, dans la suite de Fibonacci,

$$\frac{u_{n+1}}{u_n} = 1 + \frac{1}{1.1} - \frac{1}{1.2} + \frac{1}{2.3} - \frac{1}{3.5} + \frac{1}{5.8} - \ldots \pm \frac{1}{u_{n-1}u_n}.$$

Plus généralement, soient les deux formules

$$\begin{aligned} U_{n+r}V_n - U_nV_{n+r} &= 2q^nU_r, \\ V_{n+r}V_n - \Delta U_nU_{n+r} &= 2q^nV_r; \end{aligned}$$

on déduit de la première

$$\frac{U_{n+r}}{V_{n+r}} - \frac{U_n}{V_n} = 2q^n\frac{U_r}{V_nV_{n+r}};$$

remplaçons successivement, dans cette relation, n par

$$n, \quad n+r, \quad n+2r, \quad \ldots, \quad n+\overline{k-1}\,r,$$

et ajoutons les égalités obtenues, il vient

$$\frac{U_{n+kr}}{V_{n+kr}} = \frac{U_n}{V_n} + 2q^nU_r\left(\frac{1}{V_nV_{n+r}} + \frac{q^r}{V_{n+r}V_{n+2r}} + \ldots + \frac{q^{(n-1)r}}{V_{n+\overline{k-1}\,r}V_{n+kr}}\right)$$

et, de même,

$$\frac{V_{n+kr}}{U_{n+kr}} = \frac{V_n}{U_n} - 2q^nU_r\left(\frac{1}{U_nU_{n+r}} + \frac{q^r}{U_{n+r}U_{n+2r}} + \ldots + \frac{q^{(n-1)r}}{U_{n+\overline{k-1}\,r}U_{n+kr}}\right).$$

Lorsque k augmente indéfiniment, les premiers membres des égalités précédentes ont respectivement pour limites $\frac{1}{\sqrt{\Delta}}$ et $\sqrt{\Delta}$, en tenant compte des conditions de convergence. On peut ainsi développer la racine carrée d'un nombre entier en séries de fractions ayant pour numérateurs l'unité; c'était un usage familier aux savants de l'Egypte et de la Grèce. Ainsi, on a encore cette valeur approximative de $\sqrt{2}$,

$$\sqrt{2} = 1 + \frac{1}{1.3} + \frac{1}{3.4} - \frac{1}{12.34} + \varepsilon,$$

donnée par les géomètres indiens Baudhayana et Apastamba; cette valeur approximative est égale au rapport des termes $V_8 = 577$ et $U_8 = 408$ de la série de Pell. — Voir *The Çulvasûtras by* G. Thibaut, p. 13-15, dans le *Journal of the Asiatic Society of Bengal*, 1875.

Dans la théorie des fonctions circulaires, les formules précédentes correspondent aux développements de tang et de cot. On a

$$\operatorname{tang} a - \operatorname{tang} b = \frac{\sin(a-b)}{\cos a \cos b},$$

$$\cot b - \cot a = \frac{\sin(a-b)}{\sin a \sin b};$$

si l'on remplace successivement [illegible] par les termes consécutifs d'une progression arithmétique

$$[illegible]$$

on obtient facilement les sommes

$$[illegible]$$

$$[illegible]$$

Considérons encore les formules

$$[illegible]$$

on en déduit, par division,

$$[illegible]$$

Remplaçons successivement [illegible] dans la formule précédente, et ajoutons les égalités obtenues, après avoir multiplié respectivement par

$$[illegible]$$

il vient

$$[illegible]$$

Dans la théorie [illegible] devient

$$[illegible]$$

[illegible] la somme

$$[illegible] \operatorname{tang} [illegible]$$

On a la formule (n° 104, *Ex. III*)

$$\frac{z}{1-z^2}+\frac{z^2}{1-z^4}+\ldots+\frac{z^{2^{n-1}}}{1-z^{2^n}}=\frac{1}{1-z}\,\frac{z-z^{2^n}}{1-z^{2^n}};$$

si l'on y remplace z par $(b^r : a^r)$, on obtient

$$(3)\qquad \frac{q^r}{U_{2r}}+\frac{q^{2r}}{U_{4r}}+\frac{q^{4r}}{U_{8r}}+\ldots+\frac{q^{2^{n-2}r}}{U_{2^{n-1}r}}=q^r\,\frac{U_{(2^n-1)r}}{U_r\,U_{2^n r}}.$$

Plus généralement on a (n° 104, *Ex. II*)

$$q^r\,\frac{U_{(n-1)r}}{U_rU_{nr}}+q^{nr}\,\frac{U_{(n-1)nr}}{U_{nr}U_{n^2r}}+q^{n^2r}\,\frac{U_{(n-1)n^2r}}{U_{n^2r}U_{n^3r}}+\ldots+q^{n^hr}\,\frac{U_{(n-1)n^hr}}{U_{n^hr}\,U_{n^{h+1}r}}$$
$$=q^r\,\frac{U_{(n^{h+1}-1)r}}{U_r\,U_{n^{h+1}r}}.$$

Lorsque n augmente indéfiniment, le second membre de la formule (3) a pour limite $(b^r : U_r)$, dans le cas des fonctions du premier et du second genre. Par exemple, dans la suite de FIBONACCI,

$$\frac{1-\sqrt{5}}{2}=-\frac{1}{1}+\frac{1}{3}+\frac{1}{3.7}+\frac{1}{3.7.47}+\frac{1}{3.7.47.2207}+\ldots;$$

d'après les formules de duplication des arguments, chaque nouveau facteur est égal au carré du précédent, diminué de 2. De même, dans la série de PELL,

$$1-\sqrt{2}=-\frac{1}{2}+\frac{1}{2^2.3}+\frac{1}{2^3.3.17}+\frac{1}{2^4.3.17.577}+\ldots;$$

chacun des nouveaux facteurs des dénominateurs est égal au double du carré du précédent, diminué de l'unité.

Ces développements sont très rapidement convergents; c'est, en quelque sorte, la combinaison du calcul logarithmique et du calcul par les fractions continues. Ainsi le dénominateur de la trente-deuxième fraction de l'avant-dernière formule est à peu près égal à

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{2^{32}}$$

et contient *deux cent millions de chiffres*, environ. Pour écrire le dénominateur de la soixante-quatrième fraction de la formule précédente, il faudrait plus de *deux cent millions de siècles*.

LIVRE III.

LA DIVISIBILITÉ ARITHMÉTIQUE.

CHAPITRE XIX.

CODIVISEURS ET COMULTIPLES.

189. **Codiviseurs de deux nombres.** — La théorie de la divisibilité des nombres repose sur la résolution du problème suivant (EUCLIDE, Liv. VII, Prop. 2) : *Trouver tous les diviseurs communs de deux nombres entiers et positifs;* en d'autres termes, trouver tous les nombres, que nous appellerons *codiviseurs,* qui divisent à la fois deux nombres donnés, a et b. Nous observerons d'abord que si l'un des nombres est zéro, que l'on doit considérer comme multiple de tous les nombres, la recherche de tous les codiviseurs de a et de zéro revient à trouver tous les diviseurs de a, ou, ce qui revient au même, à trouver tous les codiviseurs de a et de a; mais, si les deux nombres donnés sont nuls à la fois, le problème est indéterminé, puisque tout nombre est diviseur de zéro. En exceptant ce seul cas, on démontre que les *codiviseurs de deux nombres sont les diviseurs de leur plus grand codiviseur*. Ainsi, le problème de trouver tous les codiviseurs de deux nombres inégaux revient à trouver tous les codiviseurs de deux nombres égaux à leur plus grand codiviseur, ou de trouver tous les diviseurs d'un seul nombre. On verra par la suite que ce problème est à peine connu, puisque, dans l'état actuel de la théorie des nombres, on ne connaît aucun procédé direct pour la recherche des diviseurs des nombres ayant plus de dix chiffres dans le système décimal.

Il résulte encore de cette théorie que si deux groupes de deux nombres, a et b d'une part, a' et b' d'autre part, ont le même plus grand codiviseur, ces deux groupes admettent les mêmes codiviseurs.

On dispose habituellement l'opération de la recherche du plus grand codiviseur de deux nombres, a et b, de la manière suivante :

Quotients	q_0	q_1	q_2	....	q_{n-2}	q_{n-1}	q_n	
a	b	r_1	r_2	....	r_{n-2}	r_{n-1}	r_n	
r_1	r_2	r_3	r_4	....	r_n	o	Restes	

La ligne supérieure contient les quotients des divisions successives, en nombre $(n+1)$, et la ligne inférieure contient les restes ; si l'on suppose $r_{n+1} = 0$, le plus grand codiviseur de a et b est r_n. Ce Tableau correspond aux égalités

$$
\begin{aligned}
a &= bq_0 + r_1,\\
b &= r_1 q_1 + r_2,\\
r_1 &= r_2 q_2 + r_3,\\
&\dots\dots\dots\dots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n,\\
r_{n-1} &= r_n q_n.
\end{aligned}
$$

Exemple I. — Trouver le plus grand codiviseur de deux termes consécutifs 144 et 89 de la suite de Fibonacci (n° 3).

	1	1	1	1	1	1	1	1	1	1
144	89	55	34	21	13	8	5	3	2	1
55	34	21	13	8	5	3	2	1	0	

Les quotients sont tous égaux à 1 ; les restes reforment la suite dans l'ordre décroissant, et le plus grand codiviseur est égal à l'unité.

Exemple II. — Démontrer que le nombre des termes de la suite de Fibonacci, ayant le même nombre de chiffres, est égal à 4 ou à 5.

Désignons par a le plus petit terme de la suite ayant n chiffres; le terme suivant est égal à a augmenté du nombre précédent qui est plus grand que $\frac{1}{2}a$; donc ce terme est plus grand que $\frac{3}{2}a$; par suite, les cinq termes qui suivent a sont respectivement plus grands que

$$\tfrac{3}{2}a,\quad \tfrac{5}{2}a,\quad \tfrac{8}{2}a,\quad \tfrac{13}{2}a,\quad \tfrac{21}{2}a,$$

et le dernier de ceux-ci, plus grand que $10a$, possède un chiffre de plus que a; donc il n'y a pas plus de cinq termes de n chiffres.

De même, soit b le plus grand nombre de $(n-1)$ chiffres; le nombre suivant est plus petit que $2b$; par suite, les quatre termes qui suivent b sont respectivement plus petits que

$$2b,\quad 3b,\quad 5b,\quad 8b,$$

et, par conséquent, ces quatre termes ont n chiffres. En résumé, le rang d'un terme est compris entre 4 et 5 fois le nombre de ses chiffres.

Exemple III. — Le nombre des divisions à effectuer dans la recherche du plus grand codiviseur de deux nombres ne surpasse pas le quintuple du nombre des chiffres du plus petit des deux nombres donnés.

Lorsqu'il s'agit de deux nombres consécutifs de la suite de Fibonacci, ce théorème résulte immédiatement des deux exemples précédents. Pour l'étendre à deux nombres quelconques, il suffit d'observer que, si deux restes consécutifs r_{p-1} et r_p de l'opération sont compris dans l'intervalle de deux termes consécutifs de la suite, il ne se trouve aucun reste dans l'intervalle précédent, puisque l'on a

$$r_p - r_{p+1} < u_{q+1} - u_q,$$

c'est-à-dire

$$r_{p+2} < u_{q-1};$$

cette inégalité subsiste lorsque l'un des restes est égal à l'un des termes de la suite; ainsi, le nombre des divisions ne peut surpasser le nombre des intervalles correspondants de la suite. Cet ingénieux théorème a été donné par Lamé (*Comptes rendus des séances de l'Académie des Sciences*, t. XIX, p. 867; Paris, 1853). Avant lui, le théorème avait été entrevu par Léger (*Correspondance mathématique et physique*, t. IX, p. 483) et par Finck (*Nouv. Ann. de Math.*, t. I, p. 354; 1842).

Exemple IV. — Déterminer le dernier chiffre du terme de rang n de la suite de Fibonacci.

Il suffit de connaître les derniers chiffres des quinze premiers termes et d'observer les résultats suivants : 1° les termes de rangs $(15+p)$ et $(15-p)$, pour $p \gtreqless 15$, ont leurs derniers chiffres égaux ou complémentaires à 10,

selon que p est impair ou pair; 2° les termes dont les rangs sont complémentaires à 60 ont leurs derniers chiffres complémentaires à 10; 3° les termes dont les rangs diffèrent d'un multiple de 60 ont leurs derniers chiffres égaux.

Exemple V. — Pour qu'un terme de la suite de Fibonacci soit divisible par un autre, il faut et il suffit que le rang du premier soit divisible par le rang du second.

Prenons un terme quelconque de la suite, le dixième **55**, par exemple, et considérons les termes qui le précèdent et ceux qui le suivent immédiatement, en supprimant les multiples de **55**,

$$\ldots 8,\ 13,\ 21,\ 34,\ \mathbf{0},\ 34,\ -21,\ -13,\ -8,\ \ldots;$$

nous constatons ainsi que nous reproduisons, à partir du terme **55** ou **0**, les termes de la série, pris dans l'ordre inverse, avec les signes alternés + et —. Mais la série contient le terme $u_0 = 0$; par suite, puisque **55** est le dixième terme, on retrouvera le reste 0 aux termes de rangs 20, 30, 40, ..., et non à d'autres. Ainsi, les termes de la suite, divisibles par u_n, ont pour rangs tous les multiples de n.

Remarque I. — Nous avons supposé les nombres a et b positifs; on peut aussi leur donner des signes quelconques en faisant cette convention que les diviseurs d'un nombre, ou de plusieurs nombres, sont toujours supposés positifs; mais, dans le calcul, on prend les valeurs absolues de a et de b.

Remarque II. — Dans la recherche du plus grand codiviseur de deux nombres, on peut prendre à chaque division le reste minimum, et, puisqu'il ne dépasse pas la moitié du diviseur considéré, on en déduit que, dans cette méthode, le nombre des divisions à effectuer ne surpasse pas l'exposant de la plus grande puissance de 2 contenue dans le plus petit des deux nombres a et b.

190. De deux nombres premiers entre eux. — Lorsque deux nombres sont consécutifs, tout nombre qui les divise divise leur différence, qui est l'unité; par conséquent, deux nombres consécutifs ont 1 comme unique codiviseur. En général, on dit que *deux nombres sont premiers entre eux* lorsque, dans la recherche du plus grand codiviseur, on trouve 1 comme résultat final de l'opération; on dit encore que l'un d'eux est premier à l'autre. En particulier, si l'un de ces deux nombres est 0, l'autre

est nécessairement ± 1. En faisant abstraction du diviseur 1, commun à tous les nombres, on dit encore que deux nombres premiers entre eux n'ont aucun codiviseur.

Lorsque l'on multiplie deux nombres par un troisième, le reste de la division de l'un par l'autre se trouve multiplié par ce troisième; il en est de même de tous les restes obtenus dans la recherche de leur plus grand codiviseur. De même, si l'on divise deux nombres par un de leurs facteurs communs, le reste de la division de l'un par l'autre, et leur plus grand codiviseur, sont divisés par ce troisième.

En particulier, *lorsqu'on divise deux nombres par leur plus grand codiviseur, les quotients obtenus sont premiers entre eux*. Réciproquement, si la division de deux nombres par un troisième donne des quotients premiers entre eux, le troisième nombre est le plus grand codiviseur des deux autres. On a ainsi une preuve de l'opération du plus grand codiviseur; en recommençant l'opération sur ces quotients, on doit trouver 1 pour plus grand codiviseur.

Exemple I. — Si N points sont rangés en cercle et qu'on les joigne de R en R, on passera par tous les points avant de revenir au point de départ, si R et N sont premiers entre eux.

En effet, supposons, s'il est possible, que l'on ne passe que par n points avant de revenir au point initial. Prenons un quelconque des points par lesquels on n'est pas encore passé et joignons encore de R en R; nous formerons un second polygone de n côtés n'ayant aucun sommet commun avec le premier; car, s'il en était autrement, les deux polygones coïncideraient. En faisant de même pour les points qui restent, on forme ainsi h polygones de n côtés et, puisque tous les points ont été employés une seule fois, on a $N = hn$. Mais, en joignant de R en R, chaque polygone de n côtés se trouvant fermé, on a fait un certain nombre r de fois le tour de la circonférence; on a donc $nR = rN$; il résulte des deux égalités qui précèdent

$$N = hn, \qquad R = hr;$$

par conséquent, R et N auraient un codiviseur h, ce qui est contre l'hypothèse.

Plus généralement, si N et R ont h comme plus grand codiviseur, et si l'on pose $N = hn$ et $R = hr$, on forme, en joignant les points de R en R h polygones de n côtés.

Cette démonstration a été donnée par M. MANSION dans la *Revue de l'Instruction publique en Belgique*; 1869.

Exemple II. — On considère p lignes équidistantes de q points équidistants, on a ainsi $(p-1)(q-1)$ carrés égaux; on place un point au centre de chacun de ces carrés, et l'on forme un quinconce de

$$pq+(p-1)(q-1)$$

points. Le nombre minimum de circuits continus, sans répétition ni rebroussement, pour entourer tous les points du quinconce, en les séparant l'un de l'autre, est égal au plus grand codiviseur de p et de q.

Ce curieux énoncé m'a été communiqué, en 1888, par M. BRESSON, ancien élève de l'École Polytechnique. (Voir les *Notes*, à la fin du Volume.)

191. Propriétés du plus grand codiviseur. — On a le théorème suivant : *Les restes successifs obtenus dans la recherche du plus grand codiviseur de deux nombres positifs a et b sont les différences de deux multiples de a et de b.* En d'autres termes, on a la relation

$$(1)\qquad (-1)^{p-1}r_p = ag_p - bf_p,$$

dans laquelle f_p et g_p sont deux entiers positifs. En effet, nous observerons d'abord que le théorème est immédiatement vérifié pour le premier reste r_1, puisque l'on a

$$r_1 = a - bq_0;$$

nous supposerons donc $f_1 = q_0$ et $g_1 = 1$; mais si, dans l'égalité suivante, qui définit r_2,

$$r_2 = b - r_1q_1,$$

on remplace r_1 par sa valeur, il vient

$$-r_2 = aq_1 - b(1+q_0q_1);$$

nous avons ainsi

$$f_2 = 1+q_0q_1,\qquad g_2 = q_1,$$

et les nombres f_2 et g_2 sont entiers, positifs, et respectivement plus grands que f_1 et g_1. Si nous portons les valeurs de r_1 et de r_2 dans l'égalité qui définit r_3, c'est-à-dire

$$r_3 = r_1 - r_2q_2,$$

il vient

$$+r_3 = a(1+q_1q_2) + b(q_0q_1q_2+q_2+q_0),$$

et ainsi de suite. Donc, en supposant la relation (1) vérifiée, lorsque l'on y remplace p par $(p-1)$ et par $(p-2)$, on a

$$(-1)^{p-3} r_{p-2} = ag_{p-2} - bf_{p-2},$$
$$(-1)^{p-2} r_{p-1} = ag_{p-1} - bf_{p-1};$$

si l'on porte ces valeurs de r_{p-2} et de r_{p-1} dans l'égalité qui définit r_p

$$r_p = r_{p-2} - r_{p-1} q_{p-1},$$

on retrouve la relation (1), en posant

$$(2) \qquad \begin{cases} f_p = f_{p-1} q_p + f_{p-2}, \\ g_p = g_{p-1} q_p + g_{p-2}. \end{cases}$$

Ainsi la relation (1) est démontrée. On observera que les nombres f_p et g_p sont tous entiers positifs, et croissent avec l'indice p, puisque chacun d'eux est au moins égal à la somme des deux précédents, attendu que $q_p \geqq 1$. On calcule successivement les nombres f_p et g_p, en partant des valeurs qui correspondent aux indices 1 et 2; par convention, on pose

$$f_0 = 1, \qquad g_0 = 0,$$

et il suffit alors de connaître f_1 et g_1, car la loi de récurrence s'applique encore, ainsi qu'on le constate, à partir de l'indice zéro.

Si l'on applique le théorème précédent au dernier reste r_{n-1} qui est le plus grand codiviseur δ des deux nombres positifs a et b, on en déduit ce théorème : *Le plus grand codiviseur de deux entiers positifs a et b est égal à la différence de deux multiples de a et de b.* En effet, on a pour $p = n$

$$(-1)^n \delta = ag_{n-1} - bf_{n-1}.$$

Plus particulièrement, *si a et b sont positifs et premiers entre eux, on peut trouver deux entiers positifs x et y, tels que l'on ait*

$$\pm 1 = ax - by.$$

192. Théorème d'Euclide. — *Tout nombre θ qui divise un produit de deux facteurs ab et qui est premier à l'un d'eux b divise l'autre a.*

Le résultat précédent s'applique encore pour m impair, en changeant b en $-b$, aux deux facteurs du produit

$$a + b \qquad \text{et} \qquad \frac{a^m + b^m}{a + b}.$$

Exemple V. — Si $a^\alpha + b^\beta$ est premier, le plus grand codiviseur de α et β est 1 ou une puissance de 2.

193. Codiviseurs de plusieurs nombres. — Il s'agit de déterminer tous les nombres qui divisent à la fois plusieurs nombres donnés $a, b, c, d, \ldots$. D'abord il est évident que l'ordre de succession des nombres donnés peut être pris arbitrairement ; et que, par conséquent, a et b désignent deux quelconques des nombres donnés.

Désignons par δ le plus grand codiviseur des deux nombres a et b ; nous avons vu que tout nombre qui divise a et b divise δ, et inversement tout nombre qui divise δ divise a et b. Par suite, tout nombre θ, codiviseur de $a, b, c, d, \ldots$, est un codiviseur de $\delta, c, d, \ldots$, et inversement, tout codiviseur de $\delta, c, d, \ldots$ divise les nombres donnés. Par conséquent, la recherche des codiviseurs de n nombres entiers se ramène à la recherche des codiviseurs de $(n-1)$ nombres, en remplaçant deux quelconques des nombres donnés par leur plus grand codiviseur. En appliquant ce procédé au système nouveau des $(n-1)$ nombres, on pourra remplacer celui-ci par un système de $(n-2)$ nombres, et ainsi de suite, jusqu'à ce que le système soit remplacé par un seul nombre. On a donc cette proposition : *Les codiviseurs de plusieurs nombres sont tous les diviseurs de leur plus grand codiviseur.* Mais il est bon d'observer que l'on excepte le cas où les nombres donnés sont tous nuls.

Dans la pratique, il est plus commode de rechercher le plus grand codiviseur de la manière suivante. On place les nombres donnés par ordre de grandeur croissante

$$a, \quad b, \quad c, \quad d, \quad e, \quad \ldots ;$$

on divise tous ces nombres par le plus petit d'entre eux a. On range encore dans l'ordre de grandeur les restes obtenus, en négligeant les restes nuls, et en ne conservant que l'un des restes égaux parmi plusieurs ; on obtient la suite

$$a_1, \quad b_1, \quad c_1, \quad d_1, \quad \ldots.$$

On opère sur cette suite comme sur la précédente, jusqu'à ce qu'on n'obtienne plus qu'un seul reste, qui est le plus grand codiviseur cherché. Pour légitimer ce procédé, il suffit de reprendre, en le généralisant, le raisonnement que nous avons exposé dans la recherche du plus grand codiviseur de deux nombres.

D'ailleurs, on peut, comme dans le cas de deux nombres, employer les quotients approchés par excès, ou les quotients les plus approchés, de manière à obtenir les restes les plus petits. On pourra aussi faire les simplifications dont il a été parlé ci-dessus.

Désignons par Δ le plus grand codiviseur des nombres a, b, c, d, ..., et posons

$$a = \Delta a', \quad b = \Delta b', \quad c = \Delta c', \quad d = \Delta d', \quad \ldots;$$

le plus grand codiviseur des nombres entiers a', b', c', d', ... est 1; on dit alors que les nombres n'ont aucun diviseur commun, ou sont *premiers entre eux*. Par conséquent, si l'on divise plusieurs nombres par leur plus grand codiviseur, on obtient des quotients premiers entre eux; inversement, si l'on multiplie des nombres par un nombre entier quelconque Δ, leur plus grand codiviseur est multiplié par Δ.

Il y a lieu de distinguer le cas de plusieurs nombres *premiers entre eux* du cas de plusieurs *nombres premiers deux à deux*. Il est clair que des nombres premiers deux à deux sont premiers entre eux; mais des nombres premiers entre eux ne sont pas nécessairement premiers deux à deux; ainsi, par exemple, si a, b sont deux nombres impairs premiers entre eux, les nombres a, b, $2a$, $2b$, sont premiers entre eux, mais ne le sont pas deux à deux.

194. Comultiples. — Nous allons résoudre un problème qui est en quelque sorte l'inverse du précédent. Il s'agit de trouver tous les *comultiples* de plusieurs nombres donnés ou, en d'autres termes, de trouver tous les nombres qui sont séparément divisibles par les nombres donnés. Nous démontrerons ce théorème :

Les comultiples de plusieurs nombres sont tous les multiples du plus petit de leurs comultiples.

Considérons d'abord deux nombres donnés a et b; désignons par Δ leur plus grand codiviseur, et posons

$$a = \Delta a' \quad \text{et} \quad b = \Delta b':$$

nous savons que a' et b' sont des nombres premiers entre eux. Les comultiples cherchés sont des multiples de a, et sont tous compris dans la formule ma ou $m\Delta a'$, dans laquelle m est un entier quelconque; pour que ces nombres soient des multiples de b, il faut et il suffit que $m\Delta a'$ soit multiple de $\Delta b'$, c'est-à-dire que b' divise ma'; mais b', premier avec a', divise m, et l'on a $m = m'b'$, en désignant par m' un entier quelconque. Par conséquent, tous les comultiples de a et de b sont compris dans la formule ma ou $m'a'b'\Delta$; inversement, tous les nombres compris dans cette formule sont divisibles par a ou $a'\Delta$ et b ou $b'\Delta$. On voit ainsi que tous les comultiples de deux nombres a et b sont tous les multiples d'un certain nombre

$$a'b'\Delta, \quad \text{ou} \quad \frac{ab}{\Delta},$$

que l'on appelle le *plus petit comultiple* de a et de b (¹).

Nous allons étendre cette proposition à un nombre quelconque d'entiers; il s'agit de déterminer tous les comultiples de plusieurs nombres donnés a, b, c, d, ... D'abord il est évident que l'ordre de succession des nombres donnés peut être pris arbitrairement et que, par conséquent, a et b désignent deux quelconques des nombres donnés. Désignons par μ le plus petit comultiple des deux nombres a et b; nous venons de voir que tout comultiple de ces deux nombres est un multiple de μ, et inversement. Par suite, tout nombre θ comultiple de a, b, c, d, ... est un comultiple de μ, c, d, ...; et inversement, tout comultiple de μ, c, d, ... est un multiple des nombres donnés.

Par conséquent, la recherche des comultiples de n nombres entiers se ramène à la recherche des comultiples de $(n-1)$ nombres, en remplaçant deux quelconques d'entre eux par leur plus petit comultiple. En appliquant le même procédé au système des $(n-1)$ nombres, on pourra remplacer celui-ci par un système de $(n-2)$ nombres, et ainsi de suite, jusqu'à ce que le système soit remplacé par un seul nombre, qui est le plus petit comultiple des nombres donnés.

(¹) Si deux groupes de deux nombres (a, b) et (c, d) ont le même plus grand codiviseur et le même plus petit comultiple, il n'en résulte pas, pour cela, l'identité des deux groupes. Ainsi les groupes (2, 30) et (6, 10) ont tous deux le même plus grand codiviseur 2 et le même plus petit comultiple 30.

Lorsque deux des nombres a et b sont premiers entre eux, on a $\Delta = 1$ et le plus petit comultiple des deux nombres est égal à leur produit ab; mais, d'autre part, lorsqu'un nombre c est premier à deux autres, il est premier à leur produit. Par suite :

Le plus petit comultiple de plusieurs nombres, premiers entre eux deux à deux, est égal à leur produit.

Lorsqu'un nombre est divisible par plusieurs autres, premiers entre eux deux à deux, il est divisible par leur produit.

Exemple I. — Si l'on désigne par $D(a, b, c, \ldots, l)$ le plus grand codiviseur de n nombres, par $d_1, d_2, d_3, \ldots$ les plus grands codiviseurs de groupes formés par ces nombres, de telle sorte que l'ensemble des groupes reproduise les nombres donnés, on a

$$D(a, b, c, \ldots, l) = D(d_1, d_2, d_3, \ldots).$$

Exemple II. — Si l'on désigne par $m(a, b, c, \ldots, l)$ le plus petit comultiple de n nombres, par $m_1, m_2, m_3, \ldots$ les plus petits comultiples de groupes formés par ces nombres, de telle sorte que l'ensemble des groupes reproduise les nombres donnés, on a

$$m(a, b, c, \ldots, l) = m(m_1, m_2, m_3, \ldots).$$

Exemple III. — Pour qu'un comultiple de n nombres soit le plus petit, il faut et il suffit qu'en le divisant successivement par chacun d'eux, on obtienne des quotients premiers entre eux.

Soient M un comultiple des nombres donnés et P leur produit; les produits des nombres pris $(n-1)$ à $(n-1)$ sont

$$\frac{P}{a}, \quad \frac{P}{b}, \quad \ldots, \quad \frac{P}{l};$$

cela posé, on a évidemment

$$D\left(\frac{MP}{a}, \frac{MP}{b}, \ldots, \frac{MP}{l}\right) = M.D\left(\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}\right)$$
$$= P.D\left(\frac{M}{a}, \frac{M}{b}, \ldots, \frac{M}{l}\right);$$

d'où l'on tire

$$(1) \qquad M = P\,\frac{D\left(\frac{M}{a}, \frac{M}{b}, \ldots, \frac{M}{l}\right)}{D\left(\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}\right)}.$$

Pour que M ait la plus petite valeur m, il faut et il suffit que l'on ait

$$D\left(\frac{M}{a}, \frac{M}{b}, \ldots, \frac{M}{l}\right) = 1;$$

ou, en d'autres termes, que les quotients

$$\frac{M}{a}, \frac{M}{b}, \ldots, \frac{M}{l}$$

soient premiers entre eux.

Exemple IV. — Le produit de n nombres est égal au produit de leur plus petit comultiple par le plus grand codiviseur des produits de ces nombres pris $(n-1)$ à $(n-1)$.

En effet, l'expression (1) de l'*Exemple III* donne

$$(2) \qquad P = m(a, b, \ldots, l).D\left(\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}\right).$$

Exemple V. — Le plus petit comultiple de n nombres est égal à un comultiple quelconque M divisé par le plus grand codiviseur des quotients obtenus en divisant ce comultiple par chacun des nombres.

En effet, les égalités (1) et (2) donnent

$$(3) \qquad m(a, b, c, \ldots, l) = \frac{M(a, b, \ldots, l)}{D\left(\frac{M}{a}, \frac{M}{b}, \ldots, \frac{M}{l}\right)}.$$

En supposant $M = P$, on retrouve le théorème précédent.

Exemple VI. — Le produit de n nombres est égal au produit de leur plus grand codiviseur par le plus petit comultiple des produits de ces nombres pris $(n-1)$ à $(n-1)$.

Remplaçons, dans l'égalité (3), les nombres $a, b, \ldots, l$, par $\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}$; et prenons pour M le produit P; les quotients de M par $\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}$, seront $a, b, c, \ldots$, et nous aurons

$$(4) \qquad P = m\left(\frac{P}{a}, \frac{P}{b}, \ldots, \frac{P}{l}\right).D(a, b, \ldots, l).$$

Exemple VII. — — Le produit de n nombres est égal au plus petit comultiple des produits obtenus en combinant ces nombres r à r, multiplié par le plus grand codiviseur des produits obtenus en les combinant $(n-r)$ à $(n-r)$.

Considérons les C_n^r produits des n nombres combinés r à r; le produit P est évidemment un comultiple de ces produits et les quotients obtenus en divisant P par chacun d'eux sont les C_n^{n-r} produits des nombres pris

$(n-r)$ à $(n-r)$; et il suffit d'appliquer la formule (3). On a donc la formule

$$P = m(C_n^r).D(C_n^{n-r}),$$

et en remplaçant r par $(n-r)$,

$$P = D(C_n^r).m(C_n^{n-r}).$$

Nous avons emprunté les énoncés et les démonstrations des *Exercices III* et *VII*, à un article de M. Barrieu (*Mathesis*, t. III, p. 217).

195. Codiviseurs des formes linéaires. — Nous démontrerons encore le théorème suivant sur les formes linéaires et homogènes. Considérons n formes indépendantes, et supposons, pour plus de simplicité, $n=3$. Soient

$$(1)\qquad \begin{cases} X = a_1x + b_1y + c_1z, \\ Y = a_2x + b_2y + c_2z, \\ Z = a_3x + b_3y + c_3z. \end{cases}$$

Désignons par Δ le déterminant des coefficients, et par de grandes lettres tous les mineurs. On a

$$(2)\qquad \begin{cases} \Delta x = A_1X + A_2Y + A_3Z, \\ \Delta y = B_1X + B_2Y + B_3Z, \\ \Delta z = C_1X + C_2Y + C_3Z. \end{cases}$$

D'après les relations (1), tout codiviseur de x, y, z, est aussi un codiviseur de X, Y, Z; réciproquement, par les relations (2), tout codiviseur de X, Y, Z divise x, y, z, ou divise Δ. De là, pour $\Delta = 1$, ce théorème :

Si n nombres sont premiers entre eux, il en est de même de n formes linéaires et homogènes de ces nombres, pourvu que le déterminant des coefficients soit égal à ± 1.

Le système des codiviseurs de n nombres $x, y, z, \ldots$ ne change quand on remplace ceux-ci par n fonctions linéaires et homogènes X, Y, Z, ..., de $x, y, z, \ldots$, dont le déterminant des coefficients est égal à ± 1.

Exemple I. — Si a et b ont δ pour plus grand codiviseur, les nombres $a+b$ et $a-b$ ont pour plus grand codiviseur δ ou 2δ.

Exemple II. — Considérons la suite

$$1,\ 2,\ 8,\ 50,\ 418,\ 4348,\ \ldots.$$

dans laquelle

$$u_n = (2n-1)\,u_{n-1} - (n-1)\,u_{n-2};$$

le plus grand codiviseur de u_n et u_{n-1} est 2^q, en désignant par q l'entier de $(2n+1)$ par 8 (n° **128**, *Ex. II*). (SYLVESTER).

196. Codiviseurs et comultiples des nombres fractionnaires. — On dit qu'une fraction est divisible par une autre, ou multiple d'une autre, quand elle est égale au produit de cette autre fraction par un nombre entier. Avec cette définition, les notions de codiviseurs et de comultiples s'appliquent aux nombres fractionnaires, et l'on appelle *plus grand codiviseur* de plusieurs fractions *la plus grande fraction irréductible* qui divise chacune des fractions données, et *plus petit comultiple* la plus petite fraction irréductible, qui est divisible par chacune des fractions données. Cela posé, on a le lemme suivant : Pour qu'une fraction irréductible $\frac{a}{b}$ soit divisible par une fraction irréductible $\frac{p}{q}$, il faut et il suffit que p divise a et que q soit un multiple de b. Au moyen de ce lemme, le lecteur démontrera aisément les théorèmes suivants [1] :

I. Le plus grand codiviseur de fractions irréductibles est une fraction irréductible qui a pour numérateur le plus grand codiviseur des numérateurs et pour dénominateur le plus petit comultiple des dénominateurs

$$D\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \ldots\right) = \frac{D(a_1, a_2, a_3, \ldots)}{m(b_1, b_2, b_3, \ldots)}.$$

II. Le plus petit comultiple de fractions irréductibles est une fraction irréductible qui a pour numérateur le plus petit comultiple des numérateurs et pour dénominateur le plus grand codiviseur des dénominateurs

$$m\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \ldots\right) = \frac{m(a_1, a_2, a_3, \ldots)}{D(b_1, b_2, b_3, \ldots)}.$$

III. Tout codiviseur de fractions irréductibles est un diviseur de leur plus grand codiviseur.

[1] *Voir*, pour plus de détails, un article de M. P. BARRIEU, dans le *Journal de Mathématiques élémentaires* (1884).

IV. Tout comultiple de fractions irréductibles est un multiple de leur plus petit comultiple.

V. Le produit du plus grand codiviseur de plusieurs fractions par le plus petit comultiple de leurs inverses est égal à 1.

$$D\left(\frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \cdots\right) m\left(\frac{b_1}{a_1}, \frac{b_2}{a_2}, \frac{b_3}{a_3}, \cdots\right) = 1.$$

VI. Si l'on multiplie ou si l'on divise plusieurs fractions par un même nombre, entier ou fractionnaire, leur plus grand codiviseur (ou leur plus petit comultiple), est multiplié (ou divisé) par ce nombre.

Il résulte de ces théorèmes et de quelques autres analogues que, si l'on désigne par a, b, c, ... des nombres positifs, quelconques, entiers ou fractionnaires, par P leur produit, par d et M, un codiviseur et un comultiple, par D et m le plus grand codiviseur et le plus petit comultiple, on a toujours les identités suivantes :

$$\begin{cases} D(a, b, c, \ldots) = D[D(a, b), c, \ldots], \\ m(a, b, c, \ldots) = m[m(a, b), c, \ldots]. \end{cases}$$

$$\begin{cases} D(a, b, c, \ldots).\, m\left(\frac{1}{a}, \frac{1}{b}, \frac{1}{c}, \cdots\right) = 1, \\ m(a, b, c, \ldots).\, D\left(\frac{1}{a}, \frac{1}{b}, \frac{1}{c}, \cdots\right) = 1. \end{cases}$$

$$\begin{cases} D(ak, bk, ck, \ldots) = kD(a, b, c, \ldots), \\ m(ak, bk, ck, \ldots) = km(a, b, c, \ldots). \end{cases}$$

$$\begin{cases} D(a, b, c, \ldots).\, m\left(\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \cdots\right) = M, \\ m(a, b, c, \ldots).\, D\left(\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \cdots\right) = M. \end{cases}$$

$$\begin{cases} D(a^p, b^p, c^p, \ldots) = [D(a, b, c, \ldots)]^p, \\ m(a^p, b^p, c^p, \ldots) = [m(a, b, c, \ldots)]^p. \end{cases}$$

Enfin, si l'on désigne par $m(C_n^i)$ et par $D(C_n^i)$ le plus petit comultiple et le plus grand codiviseur des produits obtenus en combinant n fractions i à i, on a

$$\begin{cases} D(C_n^i).\, m(C_n^{n-i}) = P, \\ m(C_n^i).\, D(C_n^{n-i}) = P. \end{cases}$$

CHAPITRE XX.

LES NOMBRES PREMIERS.

197. Nombres premiers. — Un nombre quelconque, en exceptant l'unité, admet au moins deux diviseurs qui sont l'unité et ce nombre lui-même; on dit qu'un nombre positif est *premier* lorsqu'il n'a d'autre diviseur que lui-même et l'unité. On dit qu'un nombre est *non premier* ou *composé* lorsqu'il admet plus de deux diviseurs. En d'autres termes, si l'on suppose la Table de Pythagore prolongée indéfiniment, les nombres premiers sont ceux qu'on ne rencontre que dans la première ligne et dans la première colonne de la Table; tous les nombres situés dans les autres lignes et les autres colonnes sont des nombres composés. Il y a donc deux espèces d'entiers positifs, les nombres premiers et les nombres composés; mais on doit observer que l'unité ne rentre dans aucune de ces deux espèces et, dans la plupart des cas, il ne convient pas de considérer l'unité comme un nombre premier, parce que les propriétés des nombres premiers ne s'appliquent pas toujours au nombre 1 (¹).

Tout nombre non premier admet au moins un diviseur premier autre que l'unité. En effet, soit n un nombre composé et soit p le plus petit des diviseurs autre que l'unité; si p n'était pas premier, il admettrait un facteur premier p' plus petit que lui qui diviserait n, multiple de p; par conséquent, p ne serait pas le plus petit diviseur de n.

Pour former une Table des nombres premiers impairs, jusqu'à une

(¹) Ainsi le nombre 1 est premier à lui-même, tandis qu'un nombre premier p n'est pas premier à lui-même; voir plus loin la théorie de l'*indicateur*. Il serait préférable de désigner tout nombre premier plus grand que 2 par le mot *simple* ou *primaire*, dans le but d'éviter ces trois expressions presque identiques qui correspondent à des idées si différentes : Les *premiers nombres*, les *nombres premiers* et les *nombres premiers entre eux*.

limite donnée, on emploie le procédé connu sous le nom de *Crible d'*ÉRATOSTHÈNE (276-194 avant J.-C.). On écrit la suite naturelle des impairs depuis 1 jusqu'à cette limite; puis on efface ceux que l'on rencontre de 3 en 3, à partir du carré de 3; on efface ensuite ceux que l'on rencontre de 5 en 5, à partir du carré de 5, en tenant compte de la place occupée par les nombres effacés; puis ceux que l'on rencontre de 7 en 7, à partir du carré de 7, et ainsi de suite en recommençant chaque fois par le carré du nombre que l'on trouve parmi les nombres restants à la suite du nombre premier dont on vient d'effacer les multiples. L'opération s'arrête d'elle-même, lorsque l'on vient d'effacer les multiples du plus grand nombre premier dont le carré est plus petit que la limite proposée.

Exemple I. — Former, par le crible, la Table des nombres premiers jusqu'à 100.

On trouve les vingt-cinq nombres premiers

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,
43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Exemple II. — Tout nombre premier plus grand que 2 est de l'une des formes linéaires $4x \pm 1$.

Tout nombre premier plus grand que 3 est de l'une des formes linéaires $6x \pm 1$.

Tout nombre premier impair est de l'une des formes $8x \pm 1$, ± 3.

Tout nombre premier plus grand que 3 est de l'une des formes $12x \pm 1$, ± 5.

Le carré d'un nombre premier plus grand que 3 est un multiple de 24 augmenté de l'unité.

Exemple III. — Tout nombre $4n+3$ est premier ou divisible par un nombre impair de nombres premiers de la même forme.

Tout nombre $6n+5$ est premier ou divisible par un nombre impair de nombres premiers de la même forme. — Il n'en est plus de même, pour les nombres des formes $8n+3$, $+5$ ou $+7$.

Exemple IV. — Le produit des n premiers nombres premiers n'est jamais la somme ou la différence de deux puissances de même exposant.

En effet, si p désigne un nombre premier impair, le binôme $a^p - b^p$ n'est pas divisible par p ou est divisible par p^2 (*Exemple IV*, n° 192). D'autre part, si p est pair et égal à $2q$, la somme $a^{2q} + b^{2q}$ n'est pas divisible par 3 et la différence $a^{2q} - b^{2q}$ n'est pas divisible par 2 ou est divisible par 8. C. Q. F. D.

En particulier, l'expression

$$2.3.5.7.11.13.17\ldots\pm 1$$

n'est jamais une puissance exacte.

198. Suite des nombres premiers. — La suite des nombres premiers est illimitée. Ce théorème important, dû à EUCLIDE, se démontre comme il suit. Soit p un nombre premier quelconque, il y a nécessairement un nombre premier plus grand que p, quel que soit p. En effet, supposons qu'on ait formé la suite de tous les nombres premiers jusqu'à p,

$$2,\quad 3,\quad 5,\quad 7,\quad 11,\quad \ldots,\quad p;$$

ajoutons l'unité au produit de tous ces nombres. Le nombre obtenu Z_p est plus grand que p et représente un nombre premier ou composé. Si Z_p est premier, le théorème est démontré; d'autre part, si Z_p n'est pas premier, il est divisible au moins par un nombre premier. Mais Z_p n'est divisible par aucun des nombres premiers 2, 3, 5, ..., p, puisque le reste de sa division par l'un de ces nombres est 1. Donc Z_p est divisible par un nombre premier plus grand que p.

On reconnaît que Z_p est premier pour $p = 3, 5, 7, 11$, tandis que pour $p = 13, 17, 19, 23$ les nombres Z_p sont composés. On a

$$\begin{aligned}
1 + 2 &= 3,\\
1 + 2.3 &= 7,\\
1 + 2.3.5 &= 31,\\
1 + 2.3.5.7 &= 211,\\
1 + 2.3.5.7.11 &= 2311,\\
1 + 2.3.5.7.11.13 &= 59.509,\\
1 + 2.3.5.7.11.13.17 &= 19.97.277,\\
1 + 2.3.5.7.11.13.17.19 &= 347.27953,\\
1 + 2.3.5.7.11.13.17.19.23 &= 317.703763.
\end{aligned}$$

Mais, dans l'état actuel de la Science, il serait très difficile de continuer cette étude et de savoir dans quels cas le nombre Z_p est premier ou composé, ou même de savoir s'il y a une série illimitée de valeurs de p donnant des nombres premiers. Cette question

paraît aussi inaccessible que les trois suivantes vérifiées jusqu'à certaines limites sur les Tables des nombres premiers :

I. Existe-t-il une infinité de groupes de deux nombres premiers dont la différence soit égale à 2?

II. Tout nombre pair est-il la somme de deux nombres premiers? Si cette dernière proposition posée par WARING (¹), dans ses *Meditationes analyticæ*, était démontrée dans le sens de l'affirmative, on en déduirait immédiatement que tout nombre impair est, de diverses manières, égal à la somme de trois nombres premiers.

III. Tout nombre pair est-il la différence de deux nombres premiers? (A. DE POLIGNAC.)

Exemple I. — Il y a une infinité de nombres premiers appartenant à la forme linéaire $(6x - 1)$.

On remplace, dans la démonstration précédente, Z_p par

$$2.3.5.7.11\ldots p - 1;$$

c'est un nombre de la forme $(6x - 1)$ qui est premier, ou divisible par un nombre premier de même forme.

Exemple II. — Il y a une infinité de nombres premiers appartenant à la forme linéaire $(4x - 1)$.

On remplace Z_p par

$$2^2.3.5.7.11\ldots p - 1;$$

c'est un nombre de la forme $(4x - 1)$ qui est premier, ou divisible par un nombre premier de même forme.

Exemple III. — En admettant le théorème, démontré plus loin, que tout diviseur premier impair d'une somme de deux carrés premiers entre eux est une somme de deux carrés, démontrer qu'il y a une infinité de nombres premiers de la forme linéaire $(4x + 1)$.

On considère l'expression

$$2^2.3^2.5^2.7^2.11^2\ldots p^2 + 1,$$

et l'on continue comme ci-dessus.

Exemple IV. — Il y a une infinité de nombres premiers de la forme linéaire $(8x + 5)$.

(¹) Dans une Lettre à GOLDBACH (30 juin 1742), publiée dans la *Correspondance mathématique et physique*, EULER écrit qu'il considère ce théorème comme tout à fait certain, quoiqu'il ne sache pas le démontrer.

En admettant le théorème de l'*Exemple III*, on considère l'expression

$$Z = 3^2.5^2.7^2.11^2 \ldots p^2 + 2^2,$$

Z étant une somme de deux carrés premiers entre eux ; tous ses diviseurs sont de la forme $(4x+1)$, c'est-à-dire de l'une des formes $(8x+1)$, $(8x+5)$; et, puisque Z est de la forme $(8x+5)$, ce nombre est premier ou divisible par un nombre premier de la même forme et plus grand que p.

Remarque. — Les théorèmes précédents sont des cas très particuliers de ce théorème remarquable énoncé par Legendre et démontré, pour la première fois, par Lejeune-Dirichlet : *Toute progression arithmétique dans laquelle deux termes consécutifs sont premiers entre eux renferme une infinité de termes qui sont des nombres premiers.* En d'autres termes, si a et b sont premiers entre eux, la forme linéaire $(ax+b)$ contient une infinité de termes qui sont des nombres premiers.

199. Distribution des nombres premiers. — Il n'existe actuellement aucune méthode pour trouver une solution satisfaisante des questions suivantes :

I. Trouver un nombre premier plus grand qu'un nombre premier donné.

II. Trouver une fonction qui ne donne que des nombres premiers.

III. Trouver le nombre premier qui suit un nombre premier donné.

IV. Trouver le nombre des nombres premiers qui ne surpassent pas un nombre donné.

V. Calculer directement le nombre premier de rang donné.

Ces questions que nous avons rangées suivant l'ordre probable de difficulté croissante paraissent encore inaccessibles, malgré les efforts des mathématiciens les plus illustres.

Fermat avait pensé, mais en annonçant qu'il n'en avait pas de démonstration, que les nombres de la forme

$$F_n = 2^{2^n} + 1,$$

étaient toujours premiers. Nous démontrerons plus loin que F_n est premier pour les valeurs de $n = 0, 1, 2, 3, 4$ et composé, pour $n = 5, 6, 12, 23, 36$ (voir n° 34).

Nous ajouterons que, pour modifier la conjecture de Fermat, on

a énoncé cette proposition : Tous les nombres qui appartiennent à la suite

$$2+1,\quad 2^2+1,\quad 2^{2^2}+1,\quad 2^{2^{2^2}}+1,\quad 2^{2^{2^{2^2}}}+1,\quad \ldots$$

sont premiers. D'autre part, EISENSTEIN a énoncé ce théorème dont il possédait probablement la démonstration : Il y a une infinité de nombres premiers de la forme $2^{2^n}+1$; mais nous ne connaissons aucune démonstration de ces deux propositions difficiles.

Consulter : *Annales de Gergonne*, t. XIX, p. 236. — *Journal de Crelle*, t. XVII, p. 87. — *Journal de Sylvester*, t. II, p. 238. — *Bulletins de l'Académie des Sciences* de Saint-Pétersbourg (nov. 1877 et janvier 1878).

Parmi plusieurs autres, EULER a donné les trois formules suivantes (*Mém.* de Berlin pour 1772, p. 36)

$$x^2+x+17,$$
$$2x^2+29,$$
$$x^2+x+41,$$

qui fournissent respectivement, pour les valeurs entières successives de x, à partir de zéro, 17, 29 et 41 nombres premiers, ainsi qu'on le vérifie facilement en calculant par différences, comme pour la Table des carrés (n° 24).

Mais ces formules, et d'autres analogues, ne peuvent représenter exclusivement des nombres premiers, car on a la proposition suivante :

Le polynôme à coefficients entiers

$$f(x)=a+bx+cx^2+dx^3+\ldots$$

ne peut donner continuellement des nombres premiers, pour toutes les valeurs entières de x.

En effet, soit $p=f(x_0)$ un nombre premier correspondant à la valeur x_0 de x; on a, quelle que soit la valeur du nombre entier y (n° 32),

$$f(x_0+py)\equiv f(x_0) \pmod{p};$$

donc $f(x_0+py)$ est divisible par p, quelque grand que soit y. Par suite, $f(x)$ ne peut représenter exclusivement des nombres premiers.

200. Décomposition d'un entier en différence de deux carrés. — Un nombre premier impair est, d'une seule manière, la différence de deux carrés. En effet, considérons l'équation

$$x^2 - y^2 = p,$$

dans laquelle p désigne un nombre premier; dans ce cas, x et y sont premiers entre eux; il en est de même de leur somme et de leur différence. On doit donc poser

$$x - y = 1, \qquad x + y = p;$$

d'où l'identité

$$\left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2 = p.$$

Mais si nous remplaçons p par le produit de deux nombres impairs p_1 et p_2 plus grands que 1, nous pourrons poser encore

$$x = \frac{p_1 + p_2}{2}, \qquad y = \frac{p_1 - p_2}{2}.$$

Ainsi, *pour qu'un nombre impair soit premier, il faut et il suffit qu'il soit, et d'une seule manière, égal à la différence des carrés de deux nombres entiers.* De là cette méthode indiquée par Fermat pour reconnaître si un nombre impair donné n est premier ou composé. On ajoute au nombre n tous les carrés jusqu'à celui de $\frac{1}{2}(n-1)$; si l'on ne trouve qu'un seul total, le dernier, égal à un carré, le nombre essayé est premier. Dans le cas contraire, le nombre est composé, et on le décompose immédiatement en un produit de deux facteurs. On simplifie considérablement le calcul en tenant compte des derniers chiffres des carrés et en se servant d'une Table de carrés (n^{os} **24** et **26**).

On a encore le théorème suivant, qui n'est qu'un cas particulier dans la théorie des formes quadratiques : *Si* A *et* B *désignent deux entiers positifs, un nombre premier* p *ne peut être donné par les deux décompositions distinctes*

$$p = \mathrm{A}a^2 + \mathrm{B}b^2, \qquad p = \mathrm{A}\alpha^2 + \mathrm{B}\beta^2.$$

En effet, on en déduirait

$$p(\beta^2 - b^2) = \mathrm{A}(a^2\beta^2 - b^2\alpha^2);$$

par suite, l'un des nombres $(a\beta \pm b\alpha)$ serait un multiple de p; mais on a l'identité

$$p^2 = (Aa\alpha \pm Bb\beta)^2 + AB(a\beta \mp b\alpha)^2.$$

Pour $AB > 1$, on doit remarquer que le carré qui multiplie AB est nul, car s'il en était autrement le second membre serait plus grand que le premier; on doit donc poser

$$\frac{a^2}{\alpha^2} = \frac{b^2}{\beta^2} = \frac{Aa^2 + Bb^2}{A\alpha^2 + B\beta^2} = 1,$$

d'où $a = \pm \alpha$, et $b = \pm \beta$.

Pour $AB = 1$, on peut supposer $a\beta \mp b\alpha = \pm p$, mais alors l'autre carré de la valeur de p^2 serait nul et l'on aurait $a = \pm \beta$ et $b = \pm \alpha$.

En partant de cette proposition et d'autres du même genre, on obtient d'autres méthodes pour la décomposition des nombres en facteurs premiers, que nous exposerons plus loin. Nous ne retiendrons ici que cette application indiquée par Sophie Germain : *Aucun nombre de la forme* $(p^4 + 4)$, *excepté* 5, *n'est un nombre premier*. En effet,

$$p^4 + 4 = (p^2)^2 + 2^2 = (p^2 - 2)^2 + 4p^2;$$

par conséquent ces nombres sont, de plusieurs manières, la somme de deux carrés. Plus généralement, on a

$$x^4 + 4y^4 = (x^2 + 2y^2)^2 - 4x^2y^2,$$

et, par suite, la décomposition

$$x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2).$$

201. Des nombres composés. — Nous avons vu (n° 197) que tout nombre non premier admet au moins un diviseur premier autre que l'unité. Cela posé, nous allons démontrer que *tout nombre qui n'est pas premier est décomposable en un produit d'un nombre fini de facteurs premiers.* — En effet, si n n'est pas premier, on peut poser

$$n = pn',$$

p désignant un nombre premier et n' un nombre premier ou com-

posé. Si n' est premier, le théorème est démontré; mais, si n' n'est pas premier, nous pourrons écrire

$$n' = p'n'',$$

p' désignant un nombre premier et n'' un nombre premier ou composé plus petit que n'. En appliquant le même raisonnement au nombre n'', et en observant que la suite des nombres entiers positifs décroissants n, n', n'', ... est limitée, on finira par trouver

$$n = pp'p''\ldots,$$

le second membre se composant d'un produit de facteurs premiers en nombre fini.

La décomposition d'un nombre en facteurs premiers n'est possible que d'une seule manière, si l'on ne tient pas compte de l'ordre des facteurs. En effet, supposons que l'on ait trouvé les deux décompositions

$$n = pp'p''\ldots \quad \text{et} \quad n = qq'q''\ldots,$$

dans lesquelles les p et les q désignent des nombres premiers. On a donc

$$(1) \qquad pp'p''\ldots = qq'q''\ldots.$$

Puisque p divise le premier membre, il divise le second; il existe nécessairement un facteur du second membre égal à p; car, si le nombre premier p n'était égal à aucun des facteurs premiers du second membre, il serait premier à chacun d'eux et à leur produit (nº 192); par suite, il ne pourrait diviser le second membre. On peut donc supposer $p = q$; puis, diviser les deux membres de l'égalité précédente par p, et obtenir l'égalité

$$p'p''\ldots = q'q''\ldots,$$

sur laquelle on recommencera le même raisonnement. Par conséquent, les facteurs du premier membre de l'égalité (1) sont respectivement égaux à ceux du second, et en nombre égal.

On simplifie la représentation d'un nombre composé n en groupant ensemble les facteurs premiers égaux. Si α, β, γ, ... désignent respectivement les nombres des facteurs égaux aux nombres

premiers inégaux deux à deux, a, b, c, ..., on aura

$$n = a^{\alpha} b^{\beta} c^{\gamma} \ldots;$$

les exposants α, β, γ, ... représentent nécessairement des nombres entiers, positifs ou nuls. En supposant $\beta = \gamma = \ldots = 0$, et $\alpha = 1$, on a simplement $n = a$, de telle sorte que la formule précédente, bien que souvent difficile à obtenir, renferme sans aucune exception tous les nombres entiers positifs, premiers ou composés, et aussi l'unité pour $a = 1$.

Exemple I. — Simplifier l'expression

$$10^{59}\left(\frac{1025}{1024}\right)^{5}\left(\frac{1048576}{1048575}\right)^{8}\left(\frac{6560}{6561}\right)^{3}\left(\frac{15624}{15625}\right)^{8}\left(\frac{9801}{9800}\right)^{4}.$$

On trouve pour résultat 2^{196}. (GAUSS.)

Exemple II. — Pour qu'un nombre soit la somme d'entiers consécutifs, il faut et il suffit qu'il ne soit pas égal à une puissance de 2.

Exemple III. — La somme des inverses des nombres premiers est infinie. En effet, on a pour $p > 1$ la série convergente

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots;$$

si l'on donne à p toutes les valeurs 2, 3, 5, 7, 11, ... des nombres premiers et si l'on multiplie les développements, tous les termes du produit sont différents ; chacun d'eux est l'inverse d'un nombre de la forme $2^{\alpha}3^{\beta}5^{\gamma}\ldots$, pour des exposants entiers, nuls ou positifs. Mais tout nombre entier n'étant décomposable en facteurs premiers que d'une seule manière, le produit

$$\frac{1}{1-\frac{1}{2}} \cdot \frac{1}{1-\frac{1}{3}} \cdot \frac{1}{1-\frac{1}{5}} \cdot \frac{1}{1-\frac{1}{7}} \cdots,$$

donne la série harmonique illimitée. Il y a donc une infinité de nombres premiers.

Cette démonstration est d'EULER. En se servant du théorème de GOLDBACH (n° 89, *Exemple X*), et du développement de $-\log\left(1-\frac{1}{p}\right)$, on démontre le théorème énoncé.

202. Suites de nombres composés consécutifs. — On peut trouver une infinité de suites formées en aussi grand nombre n qu'on

voudra d'entiers consécutifs et composés. En effet, désignons par

$$a_1, \quad a_2, \quad a_3, \quad \ldots, \quad a_n$$

n entiers consécutifs tels que le plus petit soit > 1, et cherchons n nombres consécutifs que nous pouvons désigner par

$$A + a_1, \quad A + a_2, \quad A + a_3, \quad \ldots, \quad A + a_n,$$

tels que ces nombres soient respectivement divisibles par a_1, a_2, a_3, ..., a_n. Il en résulte que A est divisible par chacun des n nombres donnés et, par suite, par leur plus petit comultiple; donc, en désignant celui-ci par μ et par t un entier quelconque, on a

$$A = t\mu.$$

Plus généralement, on peut supposer que a_1, a_2, a_3, ..., a_n désignent des nombres en progression arithmétique de raison r. Mais, si l'on veut simplement que les nombres

$$A + a_2, \quad A + a_3, \quad A + a_4, \quad \ldots, \quad A + a_n$$

soient des nombres composés, on peut remplacer μ par le produit P des nombres premiers jusqu'à n, et considérer les nombres

$$tP + 2, \quad tP + 3, \quad tP + 4, \quad \ldots, \quad tP + n;$$

ainsi, par exemple, les neuf nombres consécutifs

$$212, \quad 213, \quad 214, \quad \ldots, \quad 219, \quad 220$$

sont composés; il en sera de même, si on les augmente d'un multiple quelconque de 210.

Exemple I. — Trouver tous les nombres N qui, divisés respectivement par les nombres 2, 3, 4, ..., $(n-1)$, donnent successivement pour restes les nombres 1, 2, 3, ..., $(n-2)$.

Le nombre $(N+1)$ est évidemment divisible par 2, 3, 4, ..., $(n-1)$; par conséquent, il est divisible par leur plus petit comultiple μ; on a donc

$$N = t\mu - 1.$$

Exemple II. — Trouver tous les nombres N qui, divisés respectivement par les nombres 2, 3, 4, ..., $(n-1)$, n, donnent successivement pour restes les nombres 1, 2, 3, ..., $(n-2)$, 0.

Déterminons d'abord tous les nombres qui vérifient toutes les conditions, à l'exception de la dernière; on a, avec les notations de l'Exemple précédent,

$$N = t\mu - 1;$$

déterminons t de telle sorte que N vérifie la dernière condition; on doit donc avoir

$$t\mu - 1 = nx;$$

le problème n'est possible que pour n premier; car, sans cela, n et μ admettraient un codiviseur qui devrait diviser 1. Donc, *en supposant n premier*, μ et n sont premiers entre eux, et l'on peut déterminer deux entiers t et μ (n° 191), tels que l'on ait

$$t\mu - nx = 1.$$

Désignons par N_0 la valeur correspondante de N qui représente une première solution du problème; la différence $(X - N_0)$ doit être divisible par $2, 3, 4, \ldots, (n-1), n$; par suite, elle est divisible par leur plus petit comultiple μn. On a donc la solution générale

$$X = N_0 + \mu n y,$$

y désignant un entier quelconque.

Soit, par exemple, $n = 7$, on aura

$$X = 119 + 420y.$$

203. Divisibilité des factorielles. — Nous commencerons par résoudre le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre a qui ne surpasse pas un nombre donné n.*

Une première méthode, directe, consiste à calculer le Tableau des puissances successives de a, jusqu'à ce que l'on obtienne un exposant α tel que l'on ait

$$a^\alpha \leqq n < a^{\alpha+1},$$

et l'exposant cherché est α; on peut déterminer ainsi, par exemple, le plus grand exposant de la puissance de 2 contenue dans un nombre donné (n° 189, Remarque II).

Mais, au lieu d'employer les multiplications successives par a, on peut aussi employer les divisions successives par a. Cette méthode repose sur le théorème suivant : *Si q désigne le quotient par défaut de la division de n par a, et si q' désigne le quotient par défaut de la division de q par b, le nombre q' est égal*

au quotient par défaut de la division de n par le produit ab.
En effet, on a par définition,

$$n = aq + r, \qquad q = bq' + s,$$

r désignant l'une des valeurs $0, 1, 2, \ldots, (a-1)$, et s l'une des valeurs $0, 1, 2, \ldots, (b-1)$. On déduit

$$n = abq' + (as + r);$$

mais le nombre non négatif $(as + r)$ est au plus égal à

$$a(b-1) + (a-1) \quad \text{ou} \quad (ab-1);$$

donc q' est le quotient exact, ou approché par défaut, de la division de n par ab.

On désigne habituellement le plus grand nombre entier contenu dans $\frac{n}{a}$ par la notation $\mathrm{E}\frac{n}{a}$, que l'on prononce *entier de n par a*: on a donc

$$\mathrm{E}\frac{\mathrm{E}\frac{n}{a}}{b} = \mathrm{E}\frac{n}{ab},$$

et cette formule s'applique, en général, à l'entier de $\frac{n}{abc\ldots}$.

Cela posé, nous résoudrons le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit n! des n premiers nombres.* Les entiers qui contiennent p en facteur dans la factorielle $n!$ sont tous les multiples de p

$$p, 2p, 3p, \ldots, \mathrm{E}\frac{n}{p}p, \qquad \text{en nombre } \mathrm{E}\frac{n}{p};$$

par suite, l'exposant de p dans cette factorielle est égal à l'exposant de p dans le produit

$$1.2.3\ldots\mathrm{E}\frac{n}{p},$$

augmenté du dernier facteur. En répétant le même raisonnement sur cette nouvelle factorielle, et en appliquant le théorème précédent, il en résulte que l'exposant du nombre premier p dans la

factorielle $n!$ est égal à la somme

$$\mathrm{E}\frac{n}{p}+\mathrm{E}\frac{n}{p^2}+\mathrm{E}\frac{n}{p^3}+\ldots.$$

Lorsque n est une puissance de p, les quotients de n par $p, p^2, p^3, \ldots$, sont tous entiers, et l'on trouve pour l'exposant cherché

$$\frac{n-1}{p-1}.$$

Si l'on écrit le nombre n dans le système de numération de base p, en supposant

$$n = a + bp + cp^2 + dp^3 + \ldots,$$

on trouve facilement que l'exposant cherché a pour valeur

$$\frac{n-(a+b+c+\ldots)}{p-1},$$

et a pour limite supérieure

$$\frac{n}{p-1}.$$

Exemple I. — Quel est l'exposant de 7 dans le produit des 10000 premiers nombres?

On dispose le calcul de la manière suivante :

10000	7			
30	1428	7		
20	028	204	7	
60	0	64	29	7
4		1	1	4

et le nombre cherché est

$$1428+204+29+4=1665.$$

Exemple II. — Le produit des 1000 premiers nombres se termine par 249 zéros.

Exemple III. — Trouver le plus grand exposant de la puissance du nombre premier p contenue dans le nombre combinatoire C_m^n.

On a

$$C_m^n = \frac{m!}{n!(m-n)!},$$

et l'on applique la méthode précédente. On en déduit l'exposant de la plus haute puissance de p contenue dans le produit de n nombres consécutifs.

Exemple IV. — Trouver le plus grand exposant de la puissance d'un nombre premier p, contenue dans le produit de n nombres impairs consécutifs. — Dans le produit de n nombres en progression arithmétique.

Exemple V. — Trouver le plus petit nombre n tel que la factorielle $n!$ soit divisible par une puissance donnée p^γ d'un nombre premier p.

Voir la solution de M. Neuberg (*Mathesis*, t. VII, p. 68).

Exemple VI. — Montrer que, pour savoir combien de fois le nombre premier p est facteur dans le produit $n!$, on peut, après avoir écrit le nombre n dans le système de numération de base p, diviser par $(p-1)$ l'excès du nombre n sur la somme de ses chiffres. En conclure que p sera facteur dans le nombre combinatoire C_n^q autant de fois que, dans la soustraction de n et de q écrits dans le système de base p, il faudra ajouter p aux chiffres de n pour rendre les soustractions possibles.

204. Quotient de factorielles. — Nous allons démontrer que, si l'on a

$$n = \alpha + \beta + \gamma + \ldots + \lambda,$$

le quotient de $n!$ par le produit $\alpha!\,\beta!\,\gamma!\ldots\lambda!$ est un nombre entier; ce théorème résulte immédiatement de ce que ce nombre représente des permutations avec répétition (n° 44); mais on peut en donner une démonstration purement arithmétique.

En effet, soit p un nombre premier quelconque du dénominateur de l'expression

$$(1) \qquad \frac{n!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!};$$

l'exposant de la plus haute puissance de p contenue dans le dénominateur est égal à la somme des expressions

$$\begin{array}{l} E\frac{\alpha}{p} + E\frac{\alpha}{p^2} + E\frac{\alpha}{p^3} + \ldots, \\ E\frac{\beta}{p} + E\frac{\beta}{p^2} + E\frac{\beta}{p^3} + \ldots, \\ E\frac{\gamma}{p} + E\frac{\gamma}{p^2} + E\frac{\gamma}{p^3} + \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

et l'exposant de la plus haute puissance de p contenue dans le

numérateur est égal à

$$E\frac{n}{p} + E\frac{n}{p^2} + E\frac{n}{p^3} + \ldots.$$

Mais, par définition,

$$n = \alpha + \beta + \gamma + \ldots,$$

et, par suite,

$$E\frac{n}{p^r} > E\frac{\alpha}{p^r} + E\frac{\beta}{p^r} + E\frac{\gamma}{p^r} + \ldots;$$

par conséquent, l'exposant d'un facteur premier quelconque p du dénominateur de l'expression (1) ne surpasse jamais l'exposant du numérateur.

En particulier, le produit de n entiers consécutifs est toujours divisible par le produit $n!$ des n premiers nombres, puisque l'on a

$$\frac{(a+1)(a+2)\ldots(a+n)}{1.2\ldots n} = \frac{(a+n)!}{a!\,n!}.$$

Exemple I. — Déterminer le plus grand exposant de la puissance d'un nombre premier p contenu dans le produit des coefficients de la puissance d'un binôme.

Exemple II. — Trouver la somme des entiers par p de p termes consécutifs d'une progression arithmétique.

Exemple III. — Si $n = pq$, le produit $n!$ est divisible par $p!(q!)^p$ et aussi, en raison de la symétrie, par $q!(p!)^q$.

En effet, l'expression

$$\frac{n!}{(q!)^p}$$

est le produit des nombres combinatoires

$$C_{pq}^q C_{(p-1)q}^q \ldots C_{2q}^q C_q^q;$$

mais on a évidemment

$$C_{mq}^q = m\,C_{mq-1}^{q-1},$$

d'où l'on déduit

$$\frac{n!}{(q!)^p} = p!\,C_{pq-1}^{q-1}\,C_{(p-1)q-1}^{q-1}\ldots C_{2q-1}^{q-1}\,C_{q-1}^{q-1}.$$

Exemple IV. — Si l'on a $n = \alpha + \beta + pq + rs$, le produit $n!$ est divisible par

$$\alpha!\,\beta!\,p!\,r!\,(q!)^p(s!)^r.$$

205. Théorèmes de Tchebychef et de Polignac. — Soit n un nombre positif, entier ou fractionnaire; nous appellerons *factorielle primaire d'ordre q*, du nombre n, le produit de tous les nombres premiers dont la puissance $q^{\text{ième}}$ ne surpasse pas n, et nous désignerons ce produit par $\theta_q(n)$; en particulier, la factorielle primaire du premier ordre de n est égale au produit de tous les nombres premiers qui ne surpassent pas n. Par convention, nous écrirons

$$\theta_q(n) = 1, \qquad \text{si} \qquad n < 2^q.$$

Cela posé, on a le théorème suivant : *Le produit des factorielles primaires, de tous les ordres, pour tous les nombres*

$$\frac{n}{1}, \frac{n}{2}, \frac{n}{3}, \ldots, \frac{n}{n},$$

est égal au produit des n premiers nombres. En d'autres termes, la factorielle $n!$ est égale au produit des factorielles primaires

$$\begin{array}{llll}
\theta_1(n), & \theta_1\left(\frac{n}{2}\right), & \theta_1\left(\frac{n}{3}\right), & \ldots, \\
\theta_2(n), & \theta_2\left(\frac{n}{2}\right), & \theta_2\left(\frac{n}{3}\right), & \ldots, \\
\theta_3(n), & \theta_3\left(\frac{n}{2}\right), & \theta_3\left(\frac{n}{3}\right), & \ldots, \\
\ldots & \ldots & \ldots & \ldots ;
\end{array}$$

d'ailleurs, on s'arrête dans chaque ligne et dans chaque colonne du Tableau précédent, lorsque la factorielle primaire devient égale à 1.

En effet, chacune des factorielles primaires ne renferme un nombre premier p qu'une seule fois; cherchons l'exposant h de p dans la $q^{\text{ième}}$ ligne du Tableau

$$\theta_q(n), \quad \theta_q\left(\frac{n}{2}\right), \quad \theta_q\left(\frac{n}{3}\right), \quad \ldots, \quad \theta_q\left(\frac{n}{h}\right);$$

on aura, par définition,

$$\frac{n}{h} > p^q > \frac{n}{h+1};$$

et, par suite,

$$h \leqq \frac{n}{p^q} < h + 1;$$

c'est-à-dire

$$h = \mathrm{E}\,\frac{n}{p^q}.$$

Par conséquent, en faisant la somme des exposants de p dans chaque ligne du Tableau précédent, on trouve

$$\mathrm{E}\,\frac{n}{p} + \mathrm{E}\,\frac{n}{p^2} + \mathrm{E}\,\frac{n}{p^3} + \ldots,$$

ce qui est précisément l'exposant de p dans le produit $n!$ des n premiers nombres. C. Q. F. D.

Si l'on pose

$$\theta(n) = \theta_1(n).\theta_2(n).\theta_3(n).\theta_4(n)\ldots.$$

le théorème précédent peut s'écrire sous la forme

$$n! = \theta(n).\theta\left(\frac{n}{2}\right).\theta\left(\frac{n}{3}\right).\theta\left(\frac{n}{4}\right)\ldots.$$

Au moyen de cette formule, et en partant de deux limites du produit $n!$, que l'on déduit de la formule de Stirling, M. Tchebychef a démontré le théorème suivant, l'un des plus beaux de l'Arithmétique transcendante ([1]) : *Pour* $2a > 7$, *il y a au moins un nombre premier compris entre* a *et* $(2a - 2)$.

Comme corollaire, on a la proposition suivante (*Journal de Liouville*, 2ᵉ série, t. II) :

Le produit des n *premiers entiers ne peut être égal à une puissance d'un nombre entier, ou au produit de puissances de nombres entiers.* En effet, il y a au moins un nombre premier qui n'entre qu'une seule fois comme facteur dans le produit des n premiers nombres.

([1]) Ce théorème a été présenté en 1850 à l'Académie des Sciences de Saint-Pétersbourg. — Voir *Journal de Liouville*, t. XVII, le tome II du *Cours d'Algèbre supérieure* de Serret, et divers Mémoires de A. de Polignac, dans les *Comptes rendus de l'Académie des Sciences de Paris*.

CHAPITRE XXI.

LES DIVISEURS DES NOMBRES.

Les théories qui vont suivre supposent que les nombres que l'on considère sont *décomposés* en leurs facteurs premiers.

206. Codiviseurs et comultiples des nombres décomposés. — Nous reprendrons les problèmes que nous avons résolus pour la recherche des codiviseurs et des comultiples de plusieurs nombres, en supposant que les nombres sont décomposés. Cherchons d'abord le plus grand codiviseur de plusieurs nombres; pour cela, on considère tous les nombres premiers différents qui se trouvent dans les décompositions des nombres donnés, et l'on supprime tous ceux qui ne se trouvent point comme facteurs dans tous les nombres donnés; après cette opération, s'il ne reste aucun facteur premier, les nombres n'ont aucun codiviseur. Dans le cas contraire, soit a un nombre premier contenu dans chacun des nombres donnés; désignons par α' l'exposant choisi parmi tous les exposants de a, de telle sorte qu'il n'y en ait pas de plus petit; soient β', γ', ... les exposants de b, c, ..., choisis de la même manière; le plus grand codiviseur cherché est

$$D = a^{\alpha'} b^{\beta'} c^{\gamma'} \dots .$$

En effet, pour qu'un nombre soit divisible par un autre, il faut et il suffit que le premier contienne tous les facteurs du second avec des exposants au moins égaux à ceux qu'ils ont dans le second des nombres donnés.

On détermine d'une façon analogue le plus petit comultiple de plusieurs nombres décomposés. On prend chacun des facteurs premiers qui entrent dans l'un quelconque des nombres donnés avec un exposant égal à celui dont il est affecté dans le nombre qui le contient avec le plus grand exposant.

Exemple I. — Si un nombre est une puissance d'exposant n, les exposants des facteurs premiers qu'il contient sont des multiples de n, et réciproquement.

Exemple II. — Si le produit de plusieurs nombres premiers entre eux deux à deux est une puissance, chacun d'eux est une puissance de même exposant.

Exemple III. — Si le produit de plusieurs nombres premiers entre eux deux à deux est le double, le triple, le quadruple, le quintuple d'une puissance, l'un des facteurs est le double, le triple, le quadruple, le quintuple d'une puissance de même exposant, et les autres facteurs sont des puissances de même exposant.

Si le produit est une puissance multipliée par un nombre A contenant plusieurs facteurs premiers différents, la décomposition peut se faire de diverses manières. Ainsi, par exemple, si le produit de plusieurs nombres premiers entre eux deux à deux est le sextuple d'un carré, l'un des facteurs est le sextuple d'un carré et les autres sont des carrés; ou bien, l'un est le double d'un carré, un autre le triple d'un carré, et les autres sont des carrés.

Exemple IV. — Si l'on désigne par P_1 le produit de n nombres entiers, par P_2 le produit des plus grands codiviseurs de tous ces nombres pris deux à deux, par P_3 le produit des plus grands codiviseurs de tous ces nombres pris trois à trois, ..., par P_n le plus grand codiviseur de tous ces nombres, le plus petit comultiple m des n nombres donnés a pour expression

$$m = \frac{P_1 P_3 P_5 \dots}{P_2 P_4 P_6 \dots}.$$

Soit p un diviseur premier des nombres donnés $a, b, c, \dots, l$; désignons par $\alpha, \beta, \gamma, \dots, \lambda$ les exposants positifs ou nuls des puissances de p contenues dans ces nombres, et par e_r l'exposant de p dans P_r; si l'on suppose les nombres donnés rangés de telle sorte que les exposants $\alpha, \beta, \gamma, \dots, \lambda$ ne soient pas croissants, on voit que l'exposant e_r de p dans chacun des produits P_r est

$$\begin{aligned}
e_1 &= \alpha + \beta + \gamma + \delta + \varepsilon + \dots,\\
e_2 &= \beta + 2\gamma + 3\delta + 4\varepsilon + \dots,\\
e_3 &= \gamma + 3\delta + 6\varepsilon + \dots,\\
e_4 &= \delta + 4\varepsilon + \dots,\\
e_5 &= \varepsilon + \dots,\\
&\dots\dots\dots\dots\dots\dots,\\
&\dots\dots\dots\dots\dots\dots
\end{aligned}$$

Par conséquent, l'exposant de p dans la valeur de m, fournie par l'énoncé, est

$$e_1 - e_2 + e_3 - e_4 + e_5 - \dots :$$

et, puisque la somme alternée des coefficients du binôme est nulle, l'exposant de p dans m est égal à α.

Exemple V. — Mettre les nombres a et b sous les formes

$$a = a_1 a_2, \qquad b = b_1 b_2,$$

a_1 et b_1 n'ayant que des facteurs premiers diviseurs de a et de b, et de plus a_2 étant premier à b et b_2 premier à a.

En supposant les nombres a et b décomposés en leurs facteurs premiers, la solution est immédiate; mais on peut encore résoudre le problème sans connaître les décompositions de a et b en facteurs, par des opérations de plus grand codiviseur. Désignons par a' et b' les quotients, premiers entre eux, de a et de b par leur plus grand codiviseur D; par a'' le quotient de a' par le plus grand codiviseur A_1 de a' et de D; par a''' le quotient de a'' par le plus grand codiviseur A_2 de a'' et de A_1, et ainsi de suite, et de même pour b. On a, en supposant $A_3 = 1$ et $B_3 = 1$,

$$a = a'''.D.A_1.A_2,$$
$$b = b'''.D.B_1.B_2.$$

Exemple VI. — S'il existe des nombres entiers x, y, z qui vérifient l'équation

$$x^p + y^p + z^p = 0, \tag{1}$$

où l'on suppose p premier impair, et x, y, z premiers entre eux deux à deux, aucun des nombres x, y, z ne peut être premier ou égal à une puissance quelconque d'un nombre premier.

On a deux cas à considérer, suivant que le produit xyz est ou n'est pas divisible par p. Lorsque le produit xyz n'est pas divisible par p, on pose, d'après l'*Exemple IV* du n° 192,

$$y + z = a^p, \qquad z + x = b^p, \qquad x + y = c^p$$

et

$$\frac{y^p + z^p}{y + z} = \alpha^p, \qquad \frac{z^p + x^p}{z + x} = \beta^p, \qquad \frac{x^p + y^p}{x + y} = \gamma^p;$$

alors, on a

$$x = -a\alpha, \qquad y = -b\beta, \qquad z = -c\gamma,$$

et les nombres a et α sont premiers entre eux, ainsi que b et β, et que c et γ. On en déduit

$$2x = b^p + c^p - a^p,$$
$$2y = c^p + a^p - b^p,$$
$$2z = a^p + b^p - c^p.$$

Si l'un des nombres x, y, z est divisible par p, on peut supposer que z est divisible par p^λ et non par une puissance de p de plus grand exposant; on trouve

$$y+z=a^p, \qquad z+x=b^p, \qquad x+y=p^{\lambda p-1}c^p$$

et

$$\frac{y^p+z^p}{y+z}=\alpha^p, \qquad \frac{z^p+x^p}{z+x}=\beta^p, \qquad \frac{x^p+y^p}{x+y}=p\gamma^p;$$

alors on a

$$x=-a\alpha, \qquad y=-b\beta, \qquad z=-p^\lambda c\gamma,$$

et, par suite,

$$\begin{aligned} 2x &= p^{\lambda p-1}c^p - a^p + b^p, \\ 2y &= p^{\lambda p-1}c^p + a^p - b^p, \\ -2z &= p^{\lambda p-1}c^p - a^p - b^p. \end{aligned}$$

Les formules précédentes ont été données par LEGENDRE, dans le but de parvenir à la démonstration du fameux théorème de FERMAT, concernant l'impossibilité de résoudre l'équation (1) en nombres entiers. On trouve les mêmes formules dans la lettre d'ABEL à HOLMBOE, du 24 juin 1823 (ABEL, *Œuvres complètes*, 2e édition, t. II, p. 264 et 265).

Exemple VII. — Trouver l'exposant de la plus haute puissance d'un nombre n qui divise le produit des M premiers nombres.

Exemple VIII. — Trouver l'exposant de la plus haute puissance d'un nombre n qui divise le produit des M premiers termes d'une progression arithmétique.

207. Nombre, somme et produit des diviseurs d'un nombre décomposé. — Soit le nombre

$$n=a^\alpha b^\beta c^\gamma\ldots;$$

tout diviseur de n a pour expression

$$d=a^{\alpha'}b^{\beta'}c^{\gamma'}\ldots,$$

en supposant

α' égal à l'un des $(\alpha+1)$ nombres $0, 1, 2, \ldots, \alpha$,
β' » » $(\beta+1)$ » $0, 1, 2, \ldots, \beta$,
γ' » » $(\gamma+1)$ » $0, 1, 2, \ldots, \gamma$,
....

divisé par chacun des entiers qui le précèdent, et $\sigma(n)$ la somme des diviseurs de n, on a la formule

$$(1) \qquad S(n) + \sigma(n) = S(n-1) + 2n - 1.$$

En effet, soit α un entier plus petit que n et r_α, r'_α les restes de la division de n et de $(n-1)$ par α. Si α n'est pas un diviseur de n, on a

$$r'_\alpha = r_\alpha - 1,$$

et si α est un diviseur de n, on a $r_\alpha = 0$, par suite

$$r'_\alpha = r_\alpha - 1 + \alpha.$$

Si l'on donne à α les valeurs $1, 2, \ldots (n-1)$, et si l'on fait la somme, en observant que $r_{n-1} = 1$, on obtient la formule demandée.

Si dans la formule (1) on remplace n par $1, 2, 3, \ldots, n$, et si l'on fait la somme des égalités obtenues, on trouve

$$\sigma(1) + \sigma(2) + \sigma(3) + \ldots + \sigma(n) = n^2 - S(n).$$

208. Nombres parfaits. — On appelle *nombre parfait* un nombre égal à la somme de ses parties aliquotes. EUCLIDE a indiqué la seule méthode actuellement connue pour trouver des nombres parfaits (*Liv. IX, Prop.* 36). Soit le nombre

$$n = 2^{p-1} b,$$

dans lequel b désigne un nombre premier; en égalant à $2n$ la somme des diviseurs de n, on trouve

$$b = 2^p - 1.$$

Par suite, on obtient des nombres parfaits au moyen de la formule

$$(1) \qquad E_p = 2^{p-1}(2^p - 1),$$

mais seulement dans le cas où le second facteur est premier.

Pour que $(2^p - 1)$ soit premier, il faut que l'exposant p le soit aussi, car le binôme $(2^{pq} - 1)$ est divisible par $(2^p - 1)$ et par $(2^q - 1)$; mais, d'autre part, cette condition, qui est nécessaire, n'est pas suffisante, puisque

$$2^{11} - 1 = 23 \times 89.$$

Le Tableau suivant contient toutes les valeurs actuellement connues du nombre premier p jusqu'à 257, pour lesquelles $(2^p - 1)$

est un nombre composé ; la colonne d désigne le plus petit diviseur de ces nombres. Les résultats qui correspondent aux quatre premières valeurs de p étaient connus de FERMAT ; le facteur d pour $p = 41$ a été donné par PLANA ; les quatre suivants ont été donnés par LANDRY et les autres par M. LE LASSEUR. On les vérifie rapidement en calculant par congruences (n° 34).

p.	d.	p.	d.	p.	d.	p.	d.
11	23	47	2 351	97	11 447	211	15 193
23	47	53	6 361	113	3 391	223	18 287
29	233	59	179 951	131	263	233	1 399
37	223	73	439	151	18 121	239	479
41	13 367	79	2 687	179	359	251	503
43	431	83	167	191	383	—	—

On ne connaît aucun nombre parfait impair; mais on peut démontrer qu'*il n'existe pas d'autres nombres parfaits pairs que ceux qui sont renfermés dans la formule d'Euclide* (1). En effet, soit

$$n = 2^\alpha b^\beta c^\gamma \ldots ;$$

si n est un nombre parfait, on aura

$$2^{\alpha+1} b^\beta c^\gamma \ldots = (2^{\alpha+1} - 1)(1 + b + \ldots + b^\beta)(1 + c + \ldots + c^\gamma) \ldots$$

ou bien

$$b^\beta c^\gamma \ldots + \frac{b^\beta c^\gamma \ldots}{2^{\alpha+1} - 1} = (1 + b + \ldots + b^\beta)(1 + c + \ldots + c^\gamma) \ldots$$

Mais le second membre étant entier, il en est de même du premier membre, dont le second terme prend la forme $b^{\beta'} c^{\gamma'} \ldots$.

Par conséquent, le nombre des termes du second membre

$$(\beta + 1)(\gamma + 1) \ldots$$

doit se réduire à deux, comme le premier; ainsi, $\beta = 1$, $\gamma = 0$, $\delta = 0$, ..., et l'on trouve $n = 2^\alpha b$.

Les nombres parfaits actuellement connus correspondent à la formule

$$E_p = 2^{p-1}(2^p - 1).$$

pour les valeurs de p

2, 3, 5, 7, 13, 17, 19, 31, 61.

L'étude des nombres parfaits semble archaïque, comme celle des nombres aliquotaires et des nombres amiables, dont nous parlons plus loin. Mais on ne doit pas oublier qu'elle a donné naissance aux principaux travaux de FERMAT et, par suite, à l'Arithmétique supérieure. Au sujet des nombres parfaits impairs, DESCARTES écrivait à FRÉNICLE, le 20 décembre 1638 : « ... et je ne sais pourquoi vous jugez qu'on ne saurait parvenir par ce moyen à l'invention d'un vrai nombre parfait; que si vous avez une démonstration, j'avoue qu'elle est au delà de ma portée et que je l'estime extrêmement; car, pour moi, je juge qu'on peut trouver des nombres impairs véritablement parfaits. » (Voir n° 229, *Ex.* V et VI.)

Il reste donc à étudier la nature des nombres $(2^p - 1)$ pour les valeurs

67, 71, 89, 101, 103, 107, 109, 127, 137, 139, 149, 157,
163, 167, 173, 181, 193, 197, 199, 227, 229, 241, 257;

cependant, nous pensons avoir démontré par de très longs calculs qu'il n'existe pas de nombres parfaits pour $p = 67$ et $p = 89$.

Dans la Préface des *Cogitata physico-mathematica* (Paris, 1644), MERSENNE affirme que les nombres parfaits correspondent, en dehors des valeurs précédentes, à $p = 67$, 127, 257, et qu'il n'en existe pas d'autres pour $p < 257$; cependant, il ne donne pas la valeur $p = 61$. Quoi qu'il en soit, il résulte, de ce curieux passage, que MERSENNE était en possession d'une méthode importante dans la théorie des nombres premiers; mais cette méthode ne nous est pas parvenue.

Après avoir traité des nombres aliquotaires et des nombres amiables, MERSENNE ajoute :

« Ubi fuerit operæ pretium advertere XXVIII numeros a Petro Bungo pro perfectis exhibitos, capite XXVIII, libri de Numeris, non esse omnes perfectos, quippe 20 sunt imperfecti, adeunt solos octo perfectos habeat, videlicet

6,
28,
496,
8128,
335 50336,
85898 69056,
13 74386 91328,
2305 84300 81399 52128,

qui sunt è regione tabulæ Bungi 1, 2, 3, 4, 8, 10, 12 et 29; quique soli perfecti sunt, ut qui Bungum habuerint, errori medicinam faciant.

» Porrò numeri perfecti adeo rari sunt, ut undecim dumtaxat potuerint hactenus inveniri; hoc est, alii tres a Bungianis differentes : neque enim ullus est alius perfectus ab illis octo, nisi superes exponentem numerum 62, progressionis duplæ ab 1 incipientis. — Nonus enim perfectus est potestas exponentis 68 minus 1. — Decimus, potestas exponentis 128, minus 1. — Undecimus denique, potestas 258, minus 1, hoc est potestas 257, unitate decurtata, multiplicata per potestatem 256.

» Qui undecim alios repererit, noverit se analysim omnem, quæ fuerit hactenus, superasse : memineritque interea nullum esse perfectum à 17000 potestate ad 32000; et nullum potestatum intervallum tantum, assignari posse, quin detur illud absque perfectis. Verbi gratia, si fuerit exponens 1 050 000, nullus erit, numerus progressionis duplæ usque ad 2 090 000, qui perfectis numeris serviat, hoc est qui minor unitate, primus exstat.

» Unde clarum est quàm rari sint perfecti numeri, et quàm merito viris perfectis comparentur; esseque unam ex maximis totius Matheseos difficultatibus, præscriptam numerorum perfectorum multitudinum exhibere; quemadmodum et agnoscere num dati numeri 15, aut 20 caracteribus constantes, sint primi necne, cùm nequidem sæculum integrum huic examini, quocumque modo hactenus cognito, sufficiat. »

209. Tables de la somme des diviseurs. — Euler a donné une Table de la somme des diviseurs des premiers nombres (¹). En désignant la somme des diviseurs de n par $\sigma(n)$, on a, suivant une remarque de Descartes, pour des entiers $a, b, c, \ldots$, premiers entre eux deux à deux,

$$\sigma(abc\ldots) = \sigma(a).\sigma(b).\sigma(c)\ldots;$$

en désignant le nombre des diviseurs de n par $\nu(n)$, on a aussi, dans les mêmes conditions,

$$\nu(abc\ldots) = \nu(a).\nu(b).\nu(c)\ldots.$$

La Table d'Euler donne $\sigma(a)$, $\sigma(a^2)$, $\sigma(a^3)$, ... pour tous les nombres premiers jusqu'à 1000, et les sommes σ sont décomposées en leurs facteurs premiers. En outre, elle contient, pour les plus petites valeurs de a, les sommes $\sigma(a^\alpha)$ pour de plus grandes valeurs de a et ainsi pour $a = 2$, jusqu'à $\alpha = 36$. Ainsi ces Tables

(¹) Euler, *Op. Arith. Coll.*, I, p. 104-109 et 147.

donnent, pour diverses valeurs de a et de α, les décompositions en facteurs premiers de nombres appartenant à la forme $(a^\alpha - 1)$.

Dans l'opuscule *Observatio de summis divisorum*, qui contient des recherches très intéressantes sur la partition des nombres, Euler donne encore le Tableau de la somme des diviseurs des cent premiers nombres.

Ces Tables ont été étendues par Reuschle et surtout par Landry qui a donné toutes les décompositions de $(2^\alpha \pm 1)$, jusqu'à $\alpha \leqslant 64$, en exceptant le seul nombre $(2^{61} + 1)$. Depuis, M. Le Lasseur a appliqué une nouvelle méthode de décomposition des grands nombres en facteurs premiers, dont on retrouve l'origine dans la correspondance de Fermat. En se servant de l'identité d'Aurifeuille

$$2^{4n+2} + 1 = (2^{2n+1} + 2^{n+1} + 1)(2^{2n+1} - 2^{n+1} + 1),$$

il a reculé considérablement les limites des Tables précédentes.

210. Nombres aliquotaires. — On appelle *nombres aliquotaires* les entiers qui ont un rapport simple avec la somme de leurs parties aliquotes (n° 15). Autrefois, on appelait *nombre abondant* un entier plus petit que la somme de ses parties aliquotes, et *nombre déficient* un entier plus grand que cette somme.

Supposons que l'on veuille trouver des entiers qui soient *sous-doubles* de la somme de leurs parties aliquotes, c'est-à-dire tels que l'on ait

$$\sigma(n) = 3n;$$

si l'on prend pour n la valeur $n = 2^\alpha bcd\ldots$, dans laquelle $b, c, d, \ldots$ sont des nombres premiers impairs, inégaux deux à deux, on devra poser

$$(2^{\alpha+1} - 1)(b+1)(c+1)(d+1)\ldots = 3.2^\alpha bcd\ldots.$$

Cette équation est impossible pour $\alpha = 1$, car on en conclurait

$$(b+1)(c+1)(d+1)\ldots = 2bcd\ldots;$$

et, puisque $b, c, d, \ldots$ sont impairs, le nombre des facteurs, premiers et impairs, de n se réduirait à un seul, b, d'où l'on tirerait $b = 1$. De même pour $\alpha = 2$, on aurait

$$7(b+1)(c+1)(d+1)\ldots = 12bcd\ldots;$$

donc, en supposant $b = 7$, l'équation serait impossible par congruence pour le module 8.

En supposant $\alpha = 3$, on aura

$$5(b+1)(c+1)(d+1)\ldots = 8bcd\ldots,$$

d'où $b = 5$, $c = 3$; alors n ne peut contenir plus de deux facteurs premiers et impairs et l'on a

$$n = 2^3.3.5 = 120.$$

En supposant $\alpha = 4$, on est conduit à une impossibilité de congruence suivant le module 32; mais pour $\alpha = 5$, on trouve l'unique solution

$$n = 2^5.3.7 = 672.$$

Les hypothèses $\alpha = 6$ et $\alpha = 7$ conduisent à des impossibilités par congruences suivant le module $2^{\alpha+1}$; mais, pour $\alpha = 8$, on trouve

$$n = 2^8.5.7.19.37.73.$$

En poursuivant cette recherche, on trouve les nombres suivants qui sont sous-doubles de leurs parties aliquotes

$$2^3.3.5,$$
$$2^5.3.7,$$
$$2^8.5.7.19.37.73.$$
$$2^9.3.11.31,$$
$$2^{13}.3.11.43.127,$$
$$2^{14}.5.7.19.31.151.$$

Ces nombres se trouvent dans les écrits de Descartes et de Fermat, et, puisqu'on n'y en rencontre pas d'autres, il est probable que leur méthode de recherche ne différait pas de celle que nous venons d'exposer.

Pour trouver des nombres *sous-triples* de leurs parties aliquotes, on peut employer l'une des propositions suivantes, faciles à démontrer :

I. Si un nombre est un sous-double et n'est pas divisible par 3, son triple est un sous-triple.

II. Si un sous-double est divisible par 3, sans l'être par 5 et par 9, le produit du sous-double par 45 est un sous-triple.

III. Si un sous-double est divisible par 3, sans l'être par 7, 9 et 13, son produit par $3.7.13$ est un sous-triple.

Ainsi, on trouve en particulier les sous-triples $2^5.3^3.5.7 = 30240$ et $2^3.3^2.5.7.13 = 32760$, qui ont été donnés par **Descartes**.

Exemple I. — Vérifier que les deux nombres suivants, qui ont été indiqués par Fermat, sont des sous-quadruples

$$2^7.3^4.5.7.11^2.17.19,$$
$$2^{10}.3^4.5.7^2.11^2.19.23.89,$$
$$2^{17}.5.7^2.13.19^2.37.73.127,$$
$$2^{20}.3^3.5.7^2.13^2.19.31.61.127.337.$$

Exemple II. — Vérifier que les deux nombres suivants, qui ont été indiqués par Fermat, sont des sous-quintuples

$$2^{23}.3^7.5^3.7^4.11.13^2.17^2.31.41.61.241.307.467.2801,$$
$$2^{27}.3^5.5^3.7.11.13^2.19.29.31.43.61.113.127.$$

Exemple III. — Vérifier que les sommes des diviseurs des cubes de 7 et de 751 530 sont des carrés parfaits.

Exemple IV. — Trouver des nombres qui surpassent de deux unités la somme de leurs parties aliquotes.

Si (2^n+1) est premier, ce qui nécessite que n soit une puissance de 2, le nombre

$$2^{n-1}(2^n-1)$$

possède la propriété énoncée, et ainsi, par exemple, pour $n = 2, 4, 8, 16$.

Exemple V. — Démontrer que le plus petit nombre abondant et impair est $3^3.5.79$.

211. Nombres amiables. — On appelle ainsi un groupe de deux nombres tels que chacun d'eux soit égal à la somme des parties aliquotes de l'autre, de telle sorte que si p et q désignent ces deux nombres on a

$$\sigma(p) = \sigma(q) = p + q.$$

Pour trouver des couples de nombres amiables, on peut supposer

$$p = 2^n a, \qquad q = 2^n bc,$$

a, b, c, étant premiers impairs; par suite,

$$(2^{n+1}-1)(a+1) = (2^{n+1}-1)(b+1)(c+1) = 2^n(a+bc);$$

d'où l'on tire

$$a = bc + b + c,$$

et, en éliminant a,

$$(b - 2^n + 1)(c - 2^n + 1) = 2^{2n}.$$

Donc, pour $\alpha < n$, on en déduit

$$b = 2^n - 1 + 2^{n-\alpha},$$
$$c = 2^n - 1 + 2^{n+\alpha},$$
$$a = (2^\alpha + 1)^2 2^{2n-\alpha} - 1,$$

avec les conditions que a, b, c soient des nombres premiers ; par suite, α est impair, sans cela a serait composé.

Pour $\alpha = 1$, on trouve une première forme de nombres amiables, en supposant

$$a = 3^2.2^{2n-1} - 1,$$
$$b = 3\ .2^{n-1}\ - 1,$$
$$c = 3\ .2^n\ \ \ - 1.$$

Si l'on donne à n les valeurs successives 2, 3, 4, ..., en ne conservant que celles pour lesquelles a, b, c sont premiers, il reste les trois solutions

n.	a.	b.	c.	p.	q.
2	71	5	11	284	220
4	1151	23	47	18416	17296
7	73727	191	383	9437056	9363584.

M. Le Lasseur a constaté qu'il n'existe pas d'autres couples de nombres amiables de cette forme pour $n < 35$.

On ne peut supposer $\alpha = 3$; car, dans ce cas, l'un des nombres b ou c serait une différence de deux carrés ; il reste à étudier les cas de $\alpha = 5, 7, \ldots$, ce qui paraît assez difficile.

Euler a donné une table de 61 couples de nombres amiables ; nous citerons, en particulier, les deux nombres impairs

$$3^5.7^2.13.19.53.6959 \quad \text{et} \quad 3^5.7^2.13.19.179.2087.$$

212. Ordre et genre des nombres composés. — Nous dirons que *l'ordre* d'un nombre composé est égal à la somme des exposants des facteurs premiers qu'il contient; ainsi 1 est de l'ordre 0; tout nombre premier est de l'ordre 1; le produit de deux nombres premiers égaux ou inégaux est de l'ordre 2, et ainsi de suite. On peut d'ailleurs généraliser cette notion et remplacer les nombres premiers par un système quelconque d'entiers premiers deux à deux, en nombre limité ou illimité. Il est d'ailleurs évident que l'ordre d'un produit est égal à la somme des ordres des facteurs.

On peut se borner à ranger les nombres en deux groupes, et nous dirons qu'un nombre est du *genre* 0 ou du *genre* 1, suivant que son ordre est pair ou impair; ainsi, le genre d'un nombre quelconque s'obtient en prenant le reste du nombre qui représente l'ordre par le module 2. On comprend que l'on pourrait ranger les nombres en 3, 4, ... groupes, en prenant les restes de l'ordre suivant le module 3, 4, ... Mais, pour ce qui va suivre, nous nous bornerons à la répartition des nombres en deux groupes.

Soit un polynôme

$$A = a_0 + a_1 + a_2 + \ldots + a_\alpha,$$

composé de $(\alpha + 1)$ termes quelconques, positifs ou négatifs, mais non nuls; désignons par pos A la somme des termes positifs et par nég A, la somme des termes négatifs, pris en valeur absolue, on a évidemment

$$\text{pos}\,A + \text{nég}\,A = A.$$

Considérons un second polynôme

$$B = b_0 + b_1 + b_2 + \ldots + b_\beta,$$

nous aurons, avec des notations analogues,

$$\text{pos}\,B + \text{nég}\,B = B;$$

faisons le produit du polynôme A par les termes successifs du polynôme B, nous obtenons un polynôme contenant des termes tous dissemblables, en nombre $(\alpha + 1)(\beta + 1)$; désignons par pos AB et nég AB les sommes des termes positifs et des termes négatifs

du produit AB, on trouve facilement, par la règle des signes, les formules [1]

$$\text{pos}\,AB = \text{pos}\,A\,\text{pos}\,B + \text{nég}\,A\,\text{nég}\,B,$$
$$\text{nég}\,AB = \text{pos}\,A\,\text{nég}\,B + \text{nég}\,A\,\text{pos}\,B.$$

On a donc l'identité [2]

$$(1)\qquad \text{pos}\,AB + \varepsilon\,\text{nég}\,AB = (\text{pos}\,A + \varepsilon\,\text{nég}\,A)(\text{pos}\,B + \varepsilon\,\text{nég}\,B),$$

dans laquelle on remplace, dans le second membre développé, ε^2 par 1, en égalant ensuite les coefficients de ε et les termes qui ne le contiennent pas. Il est facile d'étendre cette formule à un nombre quelconque de polynômes A, B, C, ... Si l'on remplace ε par 1, le premier membre et chacun des facteurs du second membre de l'identité (1) représentent les sommes des termes du produit ABC... et de chacun des facteurs; si l'on remplace ε par -1, le premier membre et les facteurs du second représentent, pour chacun, la somme des termes positifs, diminuée de celle des termes négatifs. En particulier, si l'un des facteurs est nul, il en est de même du produit.

Au lieu de supposer que pos A et nég A représentent la somme des termes positifs et celle des termes négatifs, pris en valeur absolue, on peut supposer que ces symboles représentent respectivement le nombre des termes positifs et celui des termes négatifs: l'identité (1) subsiste encore. Si l'on remplace ε par 1, le premier membre et chacun des facteurs du second représentent les nombres des termes du produit et de chacun des facteurs; si l'on remplace ε par -1, le premier membre et les facteurs du second représentent, pour chacun, le nombre des termes positifs, diminué du nombre des termes négatifs. En particulier, si l'un des facteurs a un nombre égal de termes positifs et de termes négatifs, il en est de même du produit. Ce cas se présente pour les polynômes alternés d'indice α impair; mais, si tous les polynômes alternés sont d'indice pair, le nombre des termes positifs, diminué du nombre des termes négatifs, est égal à $+1$ ou à -1, suivant que le premier coefficient a_0, b_0, c_0, ... de chacun des facteurs, et celui du produit $a_0 b_0 c_0 \ldots$ est pair ou impair.

---

[1] Ces formules sont analogues à celles qui donnent $\cos(a+b)$ et $\sin(a+b)$.

[2] Cette formule est analogue à la formule de MOIVRE.

213. Classifications des diviseurs. — Soit un nombre quelconque $n = a^\alpha b^\beta c^\gamma \ldots$ décomposé en ses facteurs premiers. Si nous posons

$$
\begin{aligned}
A &= 1 + a + a^2 + \ldots + a^\alpha,\\
B &= 1 + b + b^2 + \ldots + b^\beta,\\
C &= 1 + c + c^2 + \ldots + c^\gamma,\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

nous avons vu que le produit ABC... donne tous les diviseurs de n; leur somme est égale au produit ABC.... et leur nombre est $(\alpha+1)(\beta+1)(\gamma+1)\ldots$.

Posons maintenant

$$
\begin{aligned}
A' &= 1 - a + a^2 - \ldots + (-a)^\alpha,\\
B' &= 1 - b + b^2 - \ldots + (-b)^\beta,\\
C' &= 1 - c + c^2 - \ldots + (-c)^\gamma,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots ;
\end{aligned}
$$

les termes positifs du développement du produit A'B'C'... contiennent un nombre pair de facteurs et sont du genre o; les termes négatifs contiennent un nombre impair de facteurs et sont du genre 1; en les désignant respectivement par δ_0 et par δ_1, on a donc

$$
\begin{aligned}
\Sigma\delta_0 + \Sigma\delta_1 &= ABC\ldots,\\
\Sigma\delta_0 - \Sigma\delta_1 &= A'B'C'\ldots;
\end{aligned}
$$

d'ailleurs, on a

$$
A = \frac{1 - a^{\alpha+1}}{1-a}, \qquad A' = \frac{1-(-a)^{\alpha+1}}{1+a}.
$$

D'autre part, le nombre des diviseurs δ_0, diminué du nombre des diviseurs δ_1, est égal à o ou à 1, suivant que le produit $(\alpha+1)(\beta+1)(\gamma+1)\ldots$, qui représente le nombre des diviseurs, est pair ou impair.

On peut se proposer de répartir en deux groupes tous les diviseurs d'un nombre n, qui sont les multiples d'une partie aliquote d de n. Soit $d = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$; tous les multiples de d, diviseurs de n, s'obtiennent en multipliant d par tous les diviseurs de $(n : d)$: si donc, dans les formules précédentes, on diminue respectivement les exposants $\alpha, \beta, \gamma, \ldots$ de $\alpha', \beta', \gamma', \ldots$, on obtient pour δ'_0 et δ'_1 les diviseurs de n, multiples de d, qui sont ou ne sont pas du genre de d.

On peut répartir les diviseurs d'un nombre suivant une autre méthode, en groupant tous ceux qui donnent le même résidu pour un module donné; mais cette classification repose sur la théorie des racines primitives, que nous exposons plus loin. Nous nous bornerons à la répartition des diviseurs d'un nombre impair par la considération des modules 4 et 6, et nous supposerons que, dans le second cas, le nombre considéré n'est pas divisible par 3. Désignons par A″ le nombre A ou le nombre A′, suivant que a est congru à $+1$, ou à -1, pour le module 4 (ou pour le module 6) et de même pour tous les autres facteurs premiers; désignons par f_0 et par f_1 les diviseurs du nombre n qui sont congrus à $+1$ ou à -1, pour le module considéré; on aura alors

$$\Sigma f_0 + \Sigma f_1 = \text{ABC}\ldots,$$
$$\Sigma f_0 - \Sigma f_1 = \text{A}''\text{B}''\text{C}''\ldots;$$

par addition et par soustraction, on en déduira les sommes des diviseurs f_0 et f_1.

214. Théorème de Dedekind. — Nous nous servirons des résultats qui précèdent pour établir plusieurs propositions importantes de M. Dedekind. Soit $n = a^\alpha b^\beta c^\gamma\ldots$ un nombre décomposé, et considérons le développement

$$\frac{n}{abc\ldots}(1-a)(1-b)(1-c)\ldots;$$

désignons par δ_0 et δ_1 les diviseurs qui sont du même genre que $\frac{n}{abc\ldots}$; ce produit est égal à $\Sigma\delta_0 - \Sigma\delta_1$.

Soit δ une partie aliquote de n; nous formerons tous les δ_0 et tous les δ_1 qui sont multiples de δ. On observera que les δ_0 et les δ_1 sont les multiples de $a^{\alpha-1}b^{\beta-1}c^{\gamma-1}\ldots$; par conséquent, si ces diviseurs sont aussi des multiples de δ, ce sont des multiples du plus petit comultiple de δ et de $(n : abc\ldots)$. Soit M ce plus petit comultiple; on aura

$$\text{M} = a^{\alpha'}b^{\beta'}c^{\gamma'}\ldots,$$

les différences $\alpha-\alpha'$, $\beta-\beta'$, $\gamma-\gamma'$, ... sont nulles ou égales à 1; mais l'une d'entre elles, au moins, n'est pas nulle, puisque l'on

suppose $\delta < n$. Désignons par $a, b, c, \ldots$ les nombres premiers pour lesquels cette différence n'est pas nulle : les diviseurs δ_0 et δ_1, qui sont des multiples de δ, sont donnés par le développement

$$= M(1-a)(1-b)(1-c)\ldots$$

Par conséquent, les diviseurs δ_0 et δ_1 sont en même nombre. De là ce théorème : *Si δ désigne une partie aliquote d'un nombre $n = a^\alpha b^\beta c^\gamma \ldots$, les diviseurs de n, multiples de δ et de $n : abc \ldots$, se partagent en deux groupes également nombreux, suivant qu'ils sont ou ne sont pas du genre de δ.*

On déduit de ce théorème diverses conséquences. Considérons, par exemple, la fonction $G(n)$ définie par la relation

$$(1) \qquad F(1) + F(d_1) + F(d_2) + \ldots + F(n) = G(n),$$

dans laquelle le premier membre s'applique à tous les diviseurs de n ; on en déduit la *formule inverse*

$$(2) \qquad F(n) = \Sigma G(\delta_0) - \Sigma G(\delta_1),$$

dans laquelle le signe de sommation du second membre se rapporte à toutes les valeurs de δ_0 et de δ_1 que nous venons de définir. En effet, si l'on remplace dans le second membre de l'équation (2) chacune des valeurs de δ_0 et de δ_1 par la somme des valeurs de F qui correspondent à tous les diviseurs δ de δ_0 ou de δ_1, et si l'on fait la somme des égalités obtenues, tous les termes s'annulent deux par deux, à l'exception de $F(n)$.

Supposons, par exemple, que l'on veuille déterminer l'expression de la fonction $\varphi(n)$ d'après la propriété donnée

$$(3) \qquad \varphi(1) + \varphi(d_1) + \varphi(d_2) + \ldots + \varphi(n) = n ;$$

il nous suffit de supposer $G(n) = n$, et par suite, d'après (2),

$$(4) \qquad \varphi(n) = \Sigma\delta_0 - \Sigma\delta_1 = \frac{n}{abc\ldots}(a-1)(b-1)(c-1)\ldots$$

Ainsi les formules (3) et (4) sont inverses l'une de l'autre ; et l'égalité (3) caractérise la fonction $\varphi(n)$ de n que l'on appelle l'indicateur de n (voir le Chapitre suivant).

Si l'on remplace dans la formule (1) le signe d'addition par le

signe de multiplication, on déduit de même la formule inverse

$$F(n) = \frac{\Pi G(\delta_0)}{\Pi G(\delta_1)}.$$

Prenons pour exemple la fonction arithmétique $F(n)$ telle que cette fonction soit égale à p pour n premier ou égale à une puissance d'un nombre premier, et égale à 1 lorsque n est divisible par plusieurs nombres premiers différents; on aura évidemment

$$F(1).F(d_1).F(d_2)\ldots F(d_n) = n.$$

215. Théorèmes de Liouville et de Lejeune-Dirichlet. — Désignons par x un nombre entier et positif, par $f(x)$ et $g(x)$ deux fonctions de x, et posons

$$(1) \qquad \begin{cases} F(x) = f(1) + f(2) + f(3) + \ldots + f(x), \\ G(x) = g(1) + g(2) + g(3) + \ldots + g(x). \end{cases}$$

Si $a, b, c, \ldots$, désignent tous les diviseurs de x, les nombres $\frac{x}{a}, \frac{x}{b}, \frac{x}{c}, \ldots$ représentent tous ces diviseurs dans un autre ordre. On a donc l'identité

$$(2) \qquad \begin{cases} g(a)f\left(\frac{x}{a}\right) + g(b)f\left(\frac{x}{b}\right) + g(c)f\left(\frac{x}{c}\right) + \ldots \\ = f(a)g\left(\frac{x}{a}\right) + f(b)g\left(\frac{x}{b}\right) + f(c)g\left(\frac{x}{c}\right) + \ldots. \end{cases}$$

Donnons successivement à x les valeurs $1, 2, 3, \ldots, n$ et faisons la somme des égalités obtenues. Dans la somme des premiers membres, on trouve $g(p)$ pour toutes les valeurs de x

$$p, \quad 2p, \quad 3p, \quad \ldots, \quad q_p p,$$

en désignant par q_p l'entier de $(n : p)$. Par conséquent, le coefficient de $g(p)$ dans la somme des premiers membres est $F(q_p)$.

On a donc

$$(3) \qquad \begin{cases} g(1)F(q_1) + g(2)F(q_2) + \ldots + g(n)F(q_n), \\ = f(1)G(q_1) + f(2)G(q_2) + \ldots + f(n)G(q_n). \end{cases}$$

Soit, par exemple, $g(x) = 1$ et $G(x) = x$, alors

$$(4) \quad F(q_1) + F(q_2) + \ldots + F(q_n) = q_1 f(1) + q_2 f(2) + \ldots + q_n f(n).$$

En supposant $f(x) = x$, la formule (4) donne, en désignant toujours par $\sigma(n)$ la somme des diviseurs de n,

$$(5) \qquad \sigma(1) + \sigma(2) + \ldots + \sigma(n) = q_1 + 2q_2 + \ldots + nq_n;$$

mais, en général, pq_p est le plus grand multiple de p qui ne surpasse pas n ; on a donc cette proposition : *La somme des diviseurs des n premiers entiers égale la somme des plus grands multiples de ces nombres qui ne surpassent pas n.*

La relation (5) peut s'écrire autrement ; si l'on pose

$$n = pq_p + r_p,$$

et si l'on remplace pq_p par $n - r_p$, on obtient

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) + (r_1 + r_2 + \ldots + r_n) = n^2.$$

Donc, *la somme des diviseurs des n premiers entiers, augmentée de la somme des restes que l'on obtient en divisant n par tous les entiers qui le précèdent, est égale au carré de n.*

Enfin, si dans la formule (4) on suppose $f(x) = 1$, on en déduit que *le nombre des diviseurs des n premiers entiers est égal à la somme des quotients de n par les n premiers nombres.*

Exemple I. — Démontrer les formules

$$q_1^m + q_2^m + \ldots + q_n^m = q_1 + (2^m - 1) q_2 + (3^m - 2^m) q_3 + \ldots,$$

$$\frac{1}{q_1} + \frac{1}{q_2} + \ldots + \frac{1}{q_n} = n - \frac{q_2}{1.2} - \frac{q_3}{2.3} - \frac{q_4}{3.4} - \ldots,$$

$$\frac{1}{q_1 + 1} + \frac{1}{q_2 + 1} + \ldots + \frac{1}{q_n + 1} = n - \frac{q_1}{1.2} - \frac{q_2}{2.3} - \frac{q_3}{3.4} - \ldots,$$

$$\lambda^{q_1} + \lambda^{q_2} + \ldots + \lambda^{q_n} = n + (\lambda - 1)(q_1 + \lambda q_2 + \lambda^2 q_3 + \ldots).$$

On remplace $F(x)$ successivement dans la formule (4) par

$$x^m, \quad \frac{1}{x}, \quad \frac{1}{x+1}, \quad \lambda^x.$$

On trouvera d'autres formules en remplaçant $F(x)$ par

$$\frac{1}{x(x+1)\ldots(x+\lambda)} \quad \text{et} \quad x(x+1)\ldots(x+\lambda).$$

Exemple II. — Démontrer les formules

$$q_1 q_2 q_3 \ldots q_n = \left(\frac{2}{1}\right)^{q_2} \left(\frac{3}{2}\right)^{q_3} \left(\frac{4}{3}\right)^{q_4} \cdots$$

$$(1 + q_1)(1 + q_2)\ldots(1 + q_n)\ldots = 2^{q_1 - q_2} 3^{q_2 - q_3} 4^{q_3 - q_4} \cdots .$$

On substitue à l'identité (2) une autre identité dans laquelle les signes $+$ sont remplacés par les signes $\times$; la multiplication des égalités obtenues donne l'identité

$$g(1)^{F(q_1)} g(2)^{F(q_2)} \ldots = f(1)^{G(q_1)} f(2)^{G(q_2)} \ldots ;$$

on remplace ensuite $G(x)$ par x et $F(x)$ par x, par $(1 + x)$, ...

Le lecteur trouvera un grand nombre de formules analogues aux précédentes dans l'intéressant Mémoire de M. E. Cesaro, qui a pour titre : *Excursions arithmétiques à l'infini.* Paris, 1885.

CHAPITRE XXII.

DE L'INDICATEUR.

216. De l'indicateur. — On appelle *indicateur* d'un entier positif donné n (1), le nombre des entiers de la suite

$$1, \quad 2, \quad 3, \quad \ldots, \quad n,$$

qui sont premiers à n, et l'on désigne cette fonction numérique par $\varphi(n)$. Puisque le nombre 1 est premier à lui-même, son indicateur est 1; on a, pour les premiers nombres,

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2, \quad \varphi(4) = 2, \quad \varphi(5) = 4, \quad \ldots.$$

Si a désigne un nombre premier, on a évidemment

$$\varphi(a) = a - 1,$$

et l'on observe que cette formule serait en défaut si l'on considérait 1 comme un nombre premier, tandis qu'il est essentiel de supposer $\varphi(1) = 1$, ainsi qu'on le verra plus loin (¹).

Pour qu'un nombre soit premier à n, il faut et il suffit qu'il ne contienne aucun des facteurs premiers de n; par suite, si l'on retire, de la suite donnée des n premiers nombres, tous les termes qui contiennent au moins un facteur premier de n, les autres termes représenteront les nombres premiers à n. Supposons d'abord que n ne contienne qu'un seul facteur premier a, élevé à une puissance quelconque; les nombres entiers jusqu'à n, non premiers à n, sont les multiples de a

$$a, \quad 2a, \quad 3a, \quad \ldots \quad \left(\frac{n}{a}\right)a, \qquad \text{en nombre } \frac{n}{a},$$

(¹) M. Sylvester a donné à cette fonction numérique le nom de ***totient***, et l'a désignée par $\tau(n)$. Le mot *indicateur* a été employé par Cauchy.

et les autres entiers, premiers à n, sont au nombre de

$$n - \frac{n}{a}, \quad \text{ou} \quad n\left(1 - \frac{1}{a}\right).$$

Supposons maintenant que n contienne deux facteurs premiers a et b, élevés à des puissances quelconques; les nombres non premiers à n sont les multiples de a ou de b, c'est-à-dire

$$a,\ 2a,\ 3a,\ \ldots,\ \left(\frac{n}{a}\right)a, \qquad \text{en nombre } \frac{n}{a};$$
$$b,\ 2b,\ 3b,\ \ldots,\ \left(\frac{n}{b}\right)b, \qquad \text{»} \quad \frac{n}{b};$$

mais, dans ces deux suites, il existe des nombres égaux, multiples à la fois de a et de b, et par conséquent de leur produit ab. Ainsi, les nombres comptés deux fois sont

$$ab,\ 2ab,\ 3ab,\ \ldots,\ \left(\frac{n}{ab}\right)ab, \qquad \text{en nombre } \frac{n}{ab};$$

donc, les nombres de la suite de 1 à n, qui ne contiennent ni a, ni b, c'est-à-dire ceux qui sont premiers à n, sont en nombre

$$n - \frac{n}{a} - \frac{n}{b} + \frac{n}{ab} \quad \text{ou} \quad n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right).$$

En continuant ainsi, on arrive à démontrer que, si n ne contient que les facteurs premiers $a, b, c, \ldots, l$, inégaux deux à deux, on a pour l'indicateur l'expression donnée par EULER [1]

$$(1) \qquad \varphi(n) = n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\cdots\left(1 - \frac{1}{l}\right).$$

Il reste à montrer que cette loi, trouvée par induction, est générale. Nous observerons d'abord que, si l'on désigne par q un nombre premier à n, le nombre des entiers premiers à n dans la suite des qn premiers nombres est $q\varphi(n)$, puisqu'en divisant tous ceux-ci par n, on reproduit q fois la suite des n premiers nombres.

---

(1) EULER, *Theoremata arithmetica nova methodo demonstrata* (*Comm. nov. Acta Petrop.*, t. VIII, p. 74). — *Speculationes circa quasdam insignes proprietates numerorum* (*Acta Petrop.*, t. IV, p. 18).

Soit donc N le produit par n d'une puissance quelconque d'un nombre premier L qui ne divise pas n. Les nombres de la suite des N premiers entiers qui sont premiers à n est

$$\frac{N}{n}\varphi(n). \tag{2}$$

Mais, pour obtenir les nombres de la série des N premiers entiers, qui sont premiers à N, c'est-à-dire à n et à L, il faut diminuer l'expression précédente du nombre des termes de la suite des N premiers, qui sont divisibles par L, et premiers à n; les nombres divisibles par L sont

$$L,\quad 2L,\quad 3L,\quad \ldots,\quad \left(\frac{N}{L}\right)L,$$

et pour qu'ils soient premiers à n, il faut et il suffit que leurs coefficients

$$1,\quad 2,\quad 3,\quad \ldots,\quad \frac{N}{L},$$

soient premiers à n; or, d'après la formule (2), ils sont en nombre

$$\frac{N}{nL}\varphi(n);$$

donc le nombre des entiers inférieurs et premiers à N est

$$\varphi(N) = \frac{N}{n}\varphi(n)\left(1-\frac{1}{L}\right),$$

c'est-à-dire

$$\varphi(N) = N\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{l}\right)\left(1-\frac{1}{L}\right);$$

la formule (1) est donc générale. On peut l'écrire encore sous l'une des deux formes

$$\varphi(n) = a^{\alpha-1}b^{\beta-1}c^{\gamma-1}\ldots(a-1)(b-1)(c-1)\ldots$$

ou

$$\varphi(n) = n - \sum\frac{n}{a} + \sum\frac{n}{ab} - \sum\frac{n}{abc} + \ldots.$$

Exemple I. — Vérifier par la formule d'EULER que, si p, q, r, ... désignent des entiers premiers deux à deux, on a

$$\varphi(pqr\ldots) = \varphi(p).\varphi(q).\varphi(r)\ldots.$$

Exemple II. — Démontrer directement, ou vérifier que l'indicateur d'un entier plus grand que 2 est toujours pair.

Exemple III. — Démontrer directement, ou vérifier par la formule d'Euler, les relations

$$\varphi(4n) = 2\varphi(2n),$$
$$\varphi(4n+2) = \varphi(2n+1).$$

Exemple IV. — Le nombre des fractions irréductibles plus petites que 1 et dont le dénominateur est n est égal à $\varphi(n)$.

Exemple V. — Le nombre des fractions irréductibles qui ne surpassent pas 1 et dont le dénominateur ne surpasse pas n est égal à

$$\Sigma_n \varphi(n) = 1 + \varphi(1) + \varphi(2) + \ldots + \varphi(n).$$

On peut simplifier le calcul de Σ en se servant du théorème sur l'indicateur du double d'un nombre (*Ex. III*).

Exemple VI. — Si a désigne un nombre premier et n un entier quelconque, le nombre des entiers premiers à a, qui ne surpassent pas n, est

$$n - \mathrm{E}\,\frac{n}{a}.$$

Exemple VII. — Si a et b désignent deux nombres premiers différents et n un entier quelconque, le nombre des entiers premiers à $q = a^\alpha b^\beta$, qui ne surpassent pas n, est

$$n - \mathrm{E}\,\frac{n}{a} - \mathrm{E}\,\frac{n}{b} + \mathrm{E}\,\frac{n}{ab}.$$

Exemple VIII. — Trouver la somme des entiers inférieurs et premiers à n. — En supposant $n > 2$, si q est un nombre premier à n, il en est de même de $(n-q)$, son complément à n; d'ailleurs pour n pair et > 2, le nombre $\frac{1}{2}n$ n'est pas premier à n. Donc les entiers inférieurs et premiers à n se rangent en deux groupes complémentaires pour former la somme n Ainsi, la somme cherchée est le produit de n par la moitié de son indicateur.

Exemple IX. — Si A_p désigne la somme des $p^{\text{ièmes}}$ puissances des entiers inférieurs et premiers à n, ou des produits p à p des mêmes nombres, on a l'identité symbolique

$$A^p \triangleq (n - A)^p. \qquad \text{(Cesaro.)}$$

Exemple X. — Trouver la somme des puissances semblables des nombres de la suite 1, 2, 3, ..., x, premiers à x.

Soit d un diviseur de x; on a la formule (n° 134)

$$1^{n-1}+2^{n-1}+\ldots+(x-1)^{n-1} \doteq \frac{(x+B)^n-B^n}{n},$$

$$1^{n-1}+2^{n-1}+\ldots+\left(\frac{x}{d}-1\right)^{n-1} \doteq \frac{(x+dB)^n-(dB)^n}{nd^n};$$

par un procédé analogue à celui qui conduit à l'évaluation du nombre $\varphi(x)$, on trouve, en désignant par Σ_{n-1} la somme cherchée, et par $x=a^\alpha b^\beta c^\gamma \ldots$ le nombre donné, la formule

$$n\Sigma_{n-1} \doteq (x+Q)^n-Q^n,$$

en supposant les nombres Q liés aux nombres de **Bernoulli** par les égalités

$$Q_n = B_n(1-a^{n-1})(1-b^{n-1})(1-c^{n-1})\ldots,$$

$$Q_0 = B_0\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots.$$

Ainsi, en particulier, si l'on désigne par $\pi(x)$ le produit des facteurs $a, b, c, \ldots$, de x, pris avec le signe + ou le signe —, suivant que leur nombre est pair ou impair, on a

$$2\Sigma_1 = x\varphi(x),$$
$$3\Sigma_2 = \varphi(x)\left[x^2+\tfrac{1}{2}\pi(x)\right],$$
$$4\Sigma_3 = x\varphi(x)\left[x^2+\pi(x)\right],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Par les formules de Newton (n° 151), on déduira les sommes des produits deux à deux, trois à trois, ..., de tous les nombres inférieurs et premiers à x (*Nouvelles Ann. de Math.*; 2e série, t. XVI, p. 157).

217. Table des indicateurs. — La connaissance de l'indicateur d'un nombre est d'une extrême importance pour les recherches ultérieures; il nous paraît donc indispensable de donner les diverses valeurs de ces nombres. Le Tableau suivant contient, dans une première colonne, les valeurs de l'indicateur depuis 1 jusqu'à 100; la seconde colonne n contient tous les nombres qui correspondent à cet indicateur; la troisième colonne μ contient le nombre des valeurs de n qui correspondent à l'indicateur. On remarquera la discontinuité des valeurs de l'indicateur, car il n'existe aucun nombre n dont l'indicateur $\varphi(n)$ soit égal à l'un des nombres

14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98.

Table des nombres qui correspondent à un indicateur donné jusqu'à 100.

n.	μ.
1, 2.	2
3, 4, 6.	3
5, 8, 10, 12.	4
7, 9, 14, 18.	4
15, 16, 20, 24, 30.	5
11, 22.	2
13, 21, 26, 28, 36, 42.	6
17, 32, 34, 40, 48, 60.	6
19, 27, 38, 54.	4
25, 33, 44, 50, 66.	5
23, 46.	2
35, 39, 45, 52, 56, 70, 72, 78, 84, 90.	10
29, 58.	2
31, 62.	2
51, 64, 68, 80, 96, 102, 120.	7
37, 57, 63, 74, 76, 108, 114, 126.	8
41, 55, 75, 82, 88, 100, 110, 132, 150.	9
43, 49, 86, 98.	4
69, 92, 138.	3
47, 94.	2
65, 104, 105, 112, 130, 140, 144, 156, 168, 180, 210.	11
53, 106.	2
81, 162.	2
87, 116, 174.	3
59, 118.	2
61, 77, 93, 99, 122, 124, 154, 186, 198.	9
85, 128, 136, 160, 170, 192, 204, 240.	8
67, 134.	2
71, 142.	2
73, 91, 95, 111, 117, 135, 146, 148, 152, 182, 190, 216, 222, 228, 234, 252, 270.	17
79, 158.	2
123, 164, 165, 176, 200, 220, 246, 264, 300, 330.	10
83, 166.	2
129, 147, 172, 196, 258, 294.	6
89, 115, 178, 184, 230, 276.	6
141, 188, 282.	3
97, 119, 153, 194, 195, 208, 224, 238, 260, 280, 288, 306, 312, 336, 360, 390, 420.	17
101, 125, 202, 250.	4

218. Deux extensions de l'indicateur. — On trouve une première extension de l'indicateur dans la solution de la question suivante : Parmi les n termes consécutifs d'une progression arithmétique dont la raison r est un nombre premier à n, combien y a-t-il de termes premiers à n?

Soit a le premier terme de la progression, nous pouvons remplacer les termes de celle-ci

$$(1) \qquad a, \quad a+r, \quad a+2r, \quad \ldots, \quad a+(n-1)r.$$

par les restes de leur division par n, car le plus grand codiviseur de deux nombres est égal au plus grand codiviseur de l'un d'eux n et du reste de la division de l'autre par n. Mais on démontre immédiatement la proposition fondamentale suivante :

Les restes de la division par n de n termes consécutifs d'une progression arithmétique dont la raison r est un nombre entier, premier à n, sont tous différents et reproduisent, dans un certain ordre, les nombres

$$(2) \qquad 0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad (n-1).$$

En effet, si $(a+hr)$ et $(a+kr)$, divisés par n, donnaient le même reste, leur différence

$$(k-h)r,$$

serait un multiple de n, et puisque n est premier à r, il diviserait le nombre $(k-h)$, plus petit que lui, mais qui n'est pas nul.

Par suite, le nombre des termes de la suite (1) qui sont premiers à n, est égal au nombre des termes premiers à n, dans la suite (2), et l'on a ce théorème :

Dans la suite de n termes consécutifs d'une progression arithmétique dont la raison est un nombre premier à n, le nombre des termes, premiers à n, est égal à l'indicateur de n.

D'ailleurs, en continuant la progression arithmétique, on retrouverait les restes dans le même ordre.

La seconde extension de l'indicateur répond à la solution du problème suivant : Parmi les n termes consécutifs d'une progression arithmétique dont la raison r est un nombre premier à n, déter-

miner le nombre de ces termes qui ont avec $n = d\delta$ un plus grand codiviseur égal à δ. Par des considérations analogues aux précédentes, on peut remplacer la progression (1) par la suite

$$1, \ 2, \ 3, \ \ldots, \ n;$$

mais les termes dont il s'agit sont des multiples de δ et sont égaux à

$$\delta, \ 2\delta, \ 3\delta, \ \ldots, \ d\delta.$$

D'autre part, pour que le plus grand codiviseur de $h\delta$ et de $n = d\delta$ soit égal à δ, il faut et il suffit que h et d soient premiers entre eux; par suite, le nombre demandé est égal au nombre des termes de la suite

$$1, \ 2, \ 3, \ \ldots, \ d,$$

qui sont premiers à d, c'est-à-dire égal à $\varphi(d)$. Donc, *dans une progression arithmétique de n termes consécutifs, dont la raison est un nombre premier à n, le nombre des termes qui ont avec* $n = d\delta$ *un plus grand codiviseur égal à* δ *est égal à l'indicateur de d.*

219. Indicateur d'un produit. — Nous allons démontrer directement que *l'indicateur du produit de plusieurs nombres premiers entre eux deux à deux est égal au produit des indicateurs des facteurs.* Prenons d'abord deux nombres p et q, premiers entre eux; écrivons, ainsi qu'il suit, les pq premiers nombres, et désignons $(p - 1)$ par s afin de simplifier l'écriture

$$\begin{array}{ccccccc} 1 & 2 & \ldots & h & \ldots & q \\ q+1 & q+2 & \ldots & q+h & \ldots & q+q \\ 2q+1 & 2q+2 & \ldots & 2q+h & \ldots & 2q+q \\ 3q+1 & 3q+2 & \ldots & 3q+h & \ldots & 3q+q \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ sq+1 & sq+2 & \ldots & sq+h & \ldots & sq+q. \end{array}$$

Pour que l'un des nombres de ce Tableau soit premier à pq, il faut qu'il soit séparément premier à p et premier à q. Considérons une colonne verticale quelconque, celle de rang h; si h est pre-

mier à q, il en est de même de tous les termes de la colonne, et si h n'est pas premier à q, aucun terme de cette colonne n'est premier à q. D'ailleurs la première ligne horizontale du Tableau contient $\varphi(q)$ nombres premiers à q. Mais, chacune des colonnes représente p termes consécutifs d'une progression arithmétique de raison q et nous devons y choisir les nombres premiers à p; d'après la première extension de l'indicateur, il y a, dans chacune de ces colonnes, $\varphi(p)$ nombres premiers à p; mais, comme nous ne devons prendre que les colonnes dont le rang est un nombre premier à q, le nombre des termes du Tableau (¹), premiers à pq, est donné par

$$\varphi(pq) = \varphi(p).\varphi(q).$$

Si l'on remplace q par le produit qr, les nombres p, q, r étant premiers entre eux deux à deux, on a

$$\varphi(p.qr) = \varphi(p).\varphi(qr) = \varphi(p).\varphi(q).\varphi(r),$$

et cette démonstration s'applique à un nombre quelconque de facteurs premiers entre eux deux à deux.

On retrouve ainsi une seconde démonstration de la formule d'Euler; car, si l'on suppose

$$n = a^\alpha b^\beta c^\gamma \ldots,$$

on a, par ce qui précède,

$$\varphi(n) = \varphi(a^\alpha).\varphi(b^\beta).\varphi(c^\gamma)\ldots,$$

et d'ailleurs

$$\varphi(a^\alpha) = a^{\alpha-1}(a-1), \qquad \varphi(b^\beta) = b^{\beta-1}(b-1), \qquad \ldots;$$

par suite,

$$\varphi(n) = \frac{n}{abc\ldots}(a-1)(b-1)(c-1)\ldots.$$

Considérons maintenant deux nombres p et q, contenant les mêmes facteurs premiers a, b, c, ..., avec des exposants quelcon-

---

(¹) On peut remplacer, à cause de la première extension de l'indicateur, le Tableau des pq premiers nombres par pq termes d'une progression arithmétique, pourvu que sa raison soit un nombre premier à pq.

ques, et désignons par δ le produit des premières puissances de ces facteurs. On a, par la formule précédente,

$$\begin{aligned} \delta.\varphi(p) &= p.\varphi(\delta), \\ \delta.\varphi(q) &= q.\varphi(\delta), \\ \delta.\varphi(pq) &= pq.\varphi(\delta); \end{aligned}$$

et, par suite,

$$\varphi(pq) = \varphi(p).\varphi(q).\frac{\delta}{\varphi(\delta)}.$$

Cette formule s'étend à deux nombres quelconques p_1 et q_1; alors δ désigne le produit des premières puissances des diviseurs premiers communs aux deux facteurs. Plus généralement, désignons par p, q, r, ... des entiers quelconques positifs, par δ_1 le produit des premières puissances de tous les diviseurs premiers communs à deux quelconques, et non à plus de deux, des nombres donnés; par δ_2 le produit des premières puissances de tous les diviseurs premiers communs à trois quelconques, et non à plus de trois, des nombres donnés; et ainsi de suite. On a la formule générale

$$\varphi(pqr\ldots) = \varphi(p).\varphi(q).\varphi(r)\ldots\frac{\delta_1}{\varphi(\delta_1)}\left[\frac{\delta_2}{\varphi(\delta_2)}\right]^2\left[\frac{\delta_3}{\varphi(\delta_3)}\right]^3\ldots$$

D'ailleurs, puisque, pour $\delta > 1$, l'indicateur de δ est plus petit que δ, il en résulte que l'indicateur d'un produit de plusieurs facteurs n'est jamais plus petit que le produit des indicateurs des facteurs. Pour qu'il y ait égalité, il faut et il suffit que les facteurs du produit soient premiers entre eux deux à deux.

220. Somme des indicateurs des diviseurs d'un nombre. — Supposons que l'on ait formé, dans l'ordre croissant, le tableau de tous les diviseurs

$$1,\quad \delta_1,\quad \delta_2,\quad \delta_3,\quad \ldots.\quad n,$$

d'un nombre n, et désignons par

$$n,\quad d_1,\quad d_2,\quad d_3,\quad \ldots,\quad 1,$$

les mêmes diviseurs dans l'ordre décroissant, de telle sorte que l'on ait

$$d_h\delta_h = n,$$

les nombres d_h et δ_h étant appelés *diviseurs conjugués*. Cela fait, partageons tous les nombres de la suite

$$(1) \qquad 1, \ 2, \ 3, \ \ldots, \ n,$$

en autant de classes qu'il y a de diviseurs de n. Supposons que la première classe renferme tous les termes de la suite (1) qui sont premiers à n; que la seconde classe renferme tous les termes de la suite ayant avec n le plus grand codiviseur δ_1; que la troisième classe renferme tous les termes de la suite ayant avec n le plus grand codiviseur δ_2, ..., et que la dernière classe contienne le seul nombre n ayant avec n le plus grand codiviseur n. Il est évident qu'un nombre de la suite se trouve dans l'une des classes et ne se trouve que dans une seule. Mais, d'après la seconde extension de l'indicateur, les nombres des termes de chacune des classes sont respectivement

$$\varphi(n), \quad \varphi(d_1), \quad \varphi(d_2), \quad \ldots, \quad \varphi(1),$$

et l'on a cette proposition, due à Gauss (*Disq. Arith.*, n° 39) :

La somme des indicateurs de tous les diviseurs d'un nombre est égale à ce nombre.

A cause de l'importance de la proposition précédente, nous en donnerons une seconde démonstration. Nous avons vu (n° 207), que l'on forme le tableau de tous les diviseurs d'un nombre $n = a^\alpha b^\beta c^\gamma \ldots$, en prenant les différents termes du produit ABC..., où l'on a posé

$$\begin{aligned}
A &= 1 + a + a^2 + \ldots + a^{\alpha'} + \ldots + a^\alpha, \\
B &= 1 + b + b^2 + \ldots + b^{\beta'} + \ldots + b^\beta, \\
C &= 1 + c + c^2 + \ldots + c^{\gamma'} + \ldots + c^\gamma, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Supposons que l'on forme aussi le produit $A_1 B_1 C_1 \ldots$, dans lequel on suppose

$$\begin{aligned}
A_1 &= \varphi(1) + \varphi(a) + \ldots + \varphi(a^{\alpha'}) + \ldots + \varphi(a^\alpha), \\
B_1 &= \varphi(1) + \varphi(b) + \ldots + \varphi(b^{\beta'}) + \ldots + \varphi(b^\beta), \\
C_1 &= \varphi(1) + \varphi(c) + \ldots + \varphi(c^{\gamma'}) + \ldots + \varphi(c^\gamma), \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots ;
\end{aligned}$$

un terme quelconque du premier produit ABC... a pour expression

$$a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots,$$

et le terme correspondant du second produit $A_1 B_1 C_1 \ldots$ a pour expression

$$\varphi(a^{\alpha'}).\varphi(b^{\beta'}).\varphi(c^{\gamma'})\ldots,$$

ou, par la formule de l'indicateur du produit,

$$\varphi(a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots).$$

Par conséquent, puisque le premier produit donne la somme de tous les diviseurs de n, le second produit donne la somme de tous les indicateurs des diviseurs de n; mais on a

$$A_1 = 1 + (a-1) + (a^2 - a) + \ldots + (a^\alpha - a^{\alpha-1}),$$

ou, plus simplement, puisque les termes se déduisent deux à deux,

$$A_1 = a^\alpha, \qquad B_1 = b^\beta, \qquad C_1 = c^\gamma, \qquad \ldots;$$

donc

$$A_1 B_1 C_1 \ldots = a^\alpha b^\beta c^\gamma \ldots;$$

ou, en d'autres termes, pour tous les diviseurs δ de n,

$$\sum \varphi(\delta) = n.$$

Réciproquement, toute fonction numérique Ψ, telle que l'on ait

$$\sum \Psi(\delta) = n,$$

pour tous les diviseurs d'un entier quelconque n, est identique à l'indicateur (n° **214**). En effet, si l'on suppose successivement, pour a premier,

$$n = 1,\ a,\ a^2,\ \ldots,\ a^\alpha,$$

on voit que, pour ces valeurs de n, les nombres Ψ et φ sont égaux, puisque l'on ne détermine à chaque fois qu'une seule valeur de Ψ par une formule linéaire. Puis, si l'on suppose successivement, pour a et b premiers,

$$n = ab,\ a^2 b,\ ab^2,\ a^2 b^2,\ a^3 b,\ a^3 b^2,\ a^3 b^3,\ \ldots,$$

on trouve encore $\Psi = \varphi$ pour ces valeurs de n, et ainsi de suite.

221. Troisième extension de l'indicateur. — Désignons par $\Psi(n)$ le nombre des entiers h de la suite

$$0, \ 1, \ 2, \ \ldots, \ (n-1),$$

tels que $(h-e_1), (h-e_2), \ldots, (h-e_k)$ soient des entiers premiers à n, en représentant par $e_1, e_2, \ldots, e_k$ des entiers quelconques. On a, pour deux nombres premiers entre eux, p et q, la relation

$$\Psi(p) . \Psi(q) = \Psi(pq).$$

Cette relation se démontre, comme la formule de l'indicateur, pour un produit de deux facteurs premiers entre eux; d'ailleurs, la fonction numérique Ψ devient identique à l'indicateur φ, lorsque l'on suppose $e_1 = e_2 = e_3 = \ldots = e_k = 0$.

Cela posé, soient a un nombre premier et λ le nombre des restes différents de $e_1, e_2, \ldots, e_k$, pour le module a; on trouve facilement

$$\Psi(a) = a - \lambda, \qquad \text{et} \qquad \Psi(a^\alpha) = a^{\alpha-1}(a-\lambda).$$

Supposons maintenant $n = a^\alpha b^\beta c^\gamma \ldots$; désignons par $\lambda, \mu, \nu, \ldots$, les nombres des restes différents de la suite $e_1, e_2, e_3, \ldots$, par les modules respectifs $a, b, c, \ldots$; nous aurons

$$\Psi(n) = a^{\alpha-1} b^{\beta-1} c^{\gamma-1} \ldots (a-\lambda)(b-\mu)(c-\nu) \ldots,$$

ou encore

$$\Psi(n) = \frac{n}{abc\ldots}(a-\lambda)(b-\mu)(c-\nu)\ldots.$$

En supposant $e_1 = e_2 = e_3 = \ldots = 0$, et $\lambda = \mu = \nu = \ldots = 1$, on retrouve la formule de l'indicateur.

Exemple I. — Trouver le nombre des termes de la suite

$$1.2, \ 2.3, \ 3.4, \ \ldots, \ n(n+1),$$

qui sont premiers à n.

Exemple II. — Trouver le nombre des termes de la suite

$$1.2.3, \ 2.3.4, \ 3.4.5, \ \ldots, \ n(n+1)(n+2),$$

qui sont premiers à n.

Exemple III. — Trouver le nombre des termes de la suite des triangulaires

$$\frac{1.2}{2},\quad \frac{2.3}{2},\quad \frac{3.4}{2},\quad \ldots,\quad \frac{n(n+1)}{2},$$

qui sont premiers à n.

Exemple IV. — Trouver le nombre des termes de la suite des pyramidaux

$$\frac{1.2.3}{6},\quad \frac{2.3.4}{6},\quad \frac{3.4.5}{6},\quad \ldots,\quad \frac{n(n-1)(n+2)}{6},$$

qui sont premiers à n.

Exemple V. — Soit $\varphi(a)$ le nombre des entiers non supérieurs au nombre a et premiers avec lui, et $\Psi(a, n)$ le nombre des entiers plus grands que a, premiers avec lui et non supérieurs à n, on a les formules

$$(1)\quad \Psi(1, n) + \Psi(2, n) + \ldots + \Psi(n, n) = \varphi(2) + \varphi(3) + \ldots + \varphi(n),$$

$$(2)\quad \Psi(1, n) + 2\Psi(2, n) + \ldots + (n-1)\Psi(n-1, n)$$
$$= \tfrac{1}{2}[2\varphi(2) + 3\varphi(3) + \ldots + n\varphi(n)].$$

En effet, la différence

$$\Psi(a, \nu) - \Psi(a, \nu-1)$$

a la valeur 1 ou 0, suivant que a et ν sont ou ne sont pas premiers entre eux. Remplaçons successivement a par 1, 2, ..., $(\nu-1)$ et faisons la somme, il vient

$$\sum_{a=1}^{a=\nu-1} [\Psi(a, \nu) - \Psi(a, \nu-1)] = \varphi(\nu);$$

en remplaçant ν par 2, 3, 4, ..., n, et en faisant la somme des égalités obtenues, on trouve la relation (1). On démontre de même la formule (2), en observant que la différence

$$a\Psi(a, \nu) - a\Psi(a, \nu-1)$$

prend la valeur a ou 0, suivant que a et ν sont ou ne sont pas premiers entre eux (*Nouv. Corr. math.*, t. VI, p. 267).

222. Théorèmes de M. J. Hammond. — Par la notation $\varepsilon\frac{x}{a}$, nous désignerons le nombre 1 ou 0, suivant que $\frac{x}{a}$ est ou n'est pas entier. Posons

$$(1)\qquad \nu(x) = \varepsilon\frac{x}{1} + \varepsilon\frac{x}{2} + \varepsilon\frac{x}{3} + \varepsilon\frac{x}{4} + \ldots,$$

$$(2)\qquad \sigma(x) = 1\varepsilon\frac{x}{1} + 2\varepsilon\frac{x}{2} + 3\varepsilon\frac{x}{3} + \ldots;$$

les fonctions numériques $\nu(x)$ et $\sigma(x)$ représentent respecti ment le nombre et la somme des diviseurs de x, lorsque x dési un entier positif, et s'annulent pour x fractionnaire (¹). Si x e égal au rapport de deux entiers positifs, n et m, nous obtenons

$$(3)\qquad \nu\left(\frac{n}{m}\right) = \varepsilon\frac{n}{m} + \varepsilon\frac{n}{2m} + \varepsilon\frac{n}{3m} + \ldots,$$

$$(4)\qquad \sigma\left(\frac{n}{m}\right) = \varepsilon\frac{n}{m} + 2\varepsilon\frac{n}{2m} + 3\varepsilon\frac{n}{3m} + \ldots.$$

Nous avons encore

$$(5)\qquad \sigma\left(\frac{n}{m}\right) = \frac{n}{m}\varepsilon\frac{n}{m} + \frac{n}{2m}\varepsilon\frac{n}{2m} + \frac{n}{3m}\varepsilon\frac{n}{3m} + \ldots;$$

cette formule ne diffère de la précédente qu'en ce que, dans (les diviseurs du nombre $\frac{n}{m}$, supposé entier, sont rangés dans l'or croissant, et dans (5) suivant l'ordre décroissant. D'ailleurs seconds membres de ces deux formules sont nuls pour $\frac{n}{m}$ fracti naire.

On peut exprimer l'entier de n par m, au moyen de la form

$$(6)\qquad \mathrm{E}\frac{n}{m} = \varepsilon\frac{1}{m} + \varepsilon\frac{2}{m} + \varepsilon\frac{3}{m} + \ldots + \varepsilon\frac{n}{m},$$

(¹) Lorsque p et q désignent deux entiers positifs, on peut écrire

$$\varepsilon\frac{p}{q} = \frac{1}{q}\left[1 + \cos\frac{2p\pi}{q} + \cos\frac{4p\pi}{q} + \ldots + \cos\frac{2(q-1)p\pi}{q}\right];$$

par suite

$$\varepsilon\frac{p}{q} = \varepsilon\frac{p \pm q}{q}, \qquad \varepsilon\frac{x}{a} = \varepsilon\frac{x \pm a}{a}.$$

On a donc

$$\varepsilon\frac{-p}{q} = \varepsilon\frac{p}{q}, \qquad \varepsilon\frac{0}{q} = 1.$$

Les définitions des fonctions $\nu(x)$ et $\sigma(x)$ conduisent aux formules

$$\nu(-p) = \nu(p), \qquad \sigma(-p) = \sigma(p),$$

et l'on doit considérer les valeurs de $\nu(0)$ et de $\sigma(0)$ comme infinies, comme c résulte encore de ce que tout diviseur de $-p$ est un diviseur de p, et que to nombre est un diviseur de 0.

puisque les ε du second membre, égaux à 1, sont tous multiples de m dans la suite des n premiers entiers. D'autre part, tout entier positif n est égal à la somme des indicateurs de ses diviseurs; on a donc la formule

$$(7)\qquad n = \varepsilon\frac{n}{1}\cdot\varphi(1) + \varepsilon\frac{n}{2}\cdot\varphi(2) + \varepsilon\frac{n}{3}\cdot\varphi(3) + \ldots;$$

mais on déduit de la relation (6), en remplaçant n par $n' = n - 1$,

$$\varepsilon\frac{n}{m} = \mathrm{E}\frac{n}{m} - \mathrm{E}\frac{n'}{m};$$

par suite, la relation (7) devient

$$\begin{aligned} n = {} & \mathrm{E}\frac{n}{1}\cdot\varphi(1) + \mathrm{E}\frac{n}{2}\cdot\varphi(2) + \mathrm{E}\frac{n}{3}\cdot\varphi(3) + \ldots + \mathrm{E}\frac{n}{n}\cdot\varphi(n) \\ & - \mathrm{E}\frac{n'}{1}\cdot\varphi(1) - \mathrm{E}\frac{n'}{2}\cdot\varphi(2) - \mathrm{E}\frac{n'}{3}\cdot\varphi(3) - \ldots - \mathrm{E}\frac{n'}{n'}\cdot\varphi(n'). \end{aligned}$$

En remplaçant successivement n par 1, 2, 3, ..., n, et en faisant la somme des égalités obtenues, il vient

$$(8)\quad \frac{1}{2}n(n+1) = \mathrm{E}\frac{n}{1}\cdot\varphi(1) + \mathrm{E}\frac{n}{2}\cdot\varphi(2) + \mathrm{E}\frac{n}{3}\cdot\varphi(3) + \ldots + \mathrm{E}\frac{n}{n}\cdot\varphi(n).$$

Si l'on remplace n successivement par 1, 2, 3, ..., n dans la formule (7), on obtient un système (A) d'équations linéaires qui donne

$$(9)\qquad \varphi(n) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & \ldots & 1 \\ 1 & 1 & 0 & 0 & 0 & \ldots & 2 \\ 1 & 0 & 1 & 0 & 0 & \ldots & 3 \\ 1 & 1 & 0 & 1 & 0 & \ldots & 4 \\ 1 & 0 & 0 & 0 & 1 & \ldots & 5 \\ 1 & 1 & 1 & 0 & 0 & \ldots & 6 \\ . & . & . & . & . & \ldots & . \\ . & . & . & . & . & \ldots & . \end{vmatrix}.$$

On exprime ainsi $\varphi(n)$ par un déterminant d'ordre n dans lequel la dernière colonne contient les n premiers entiers; dans les $(n-1)$ premières colonnes, tout élément a_r^s est égal à $\varepsilon\frac{r}{s}$, c'est-à-dire à 1 ou à 0, suivant que r est ou n'est pas divisible

par s. Ainsi, la colonne de rang s se compose de $(s-1)$ zéros, suivis de 1, autant de fois que possible.

De même, la formule (8) donne

$$(10)\qquad \varphi(n) = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & \ldots & 1 \\ 2 & 1 & 0 & 0 & 0 & \ldots & 3 \\ 3 & 1 & 1 & 0 & 0 & \ldots & 6 \\ 4 & 2 & 1 & 1 & 0 & \ldots & 10 \\ 5 & 2 & 1 & 1 & 1 & \ldots & 15 \\ 6 & 3 & 2 & 1 & 1 & \ldots & 21 \\ . & . & . & . & . & \ldots & .. \\ . & . & . & . & . & \ldots & .. \end{vmatrix}.$$

La dernière colonne contient les n premiers triangulaires ; pour les autres, la colonne de rang s se compose d'abord de $(s-1)$ zéros, puis de s éléments égaux à 1, puis à 2, à 3, ..., aussi loin que possible. D'ailleurs, le déterminant (10) se déduit du déterminant (9) en ajoutant aux éléments d'une ligne de celui-ci tous les éléments des lignes précédentes.

Exemple I. — Démontrer la formule

$$\sigma(n) = \nu\left(\frac{n}{1}\right)\cdot\varphi(1) + \nu\left(\frac{n}{2}\right)\cdot\varphi(2) + \nu\left(\frac{n}{3}\right)\cdot\varphi(3) + \ldots + \nu\left(\frac{n}{n}\right)\cdot\varphi(n).$$

Il suffit de multiplier respectivement les équations du système (A), déduit de la formule (7), par

$$\varepsilon\frac{n}{1},\quad \varepsilon\frac{n}{2},\quad \varepsilon\frac{n}{3},\quad \ldots,\quad \varepsilon\frac{n}{n},$$

et d'ajouter en tenant compte des relations (2) et (3).

Exemple II. — Démontrer la formule

$$n\nu(n) = \sigma\left(\frac{n}{1}\right)\cdot\varphi(1) - \sigma\left(\frac{n}{2}\right)\cdot\varphi(2) + \sigma\left(\frac{n}{3}\right)\cdot\varphi(3) + \ldots + \sigma\left(\frac{n}{n}\right)\cdot\varphi(n).$$

Il suffit de multiplier respectivement les équations du système (A) par

$$\frac{n}{1}\varepsilon\frac{n}{1},\quad \frac{n}{2}\varepsilon\frac{n}{2},\quad \frac{n}{3}\varepsilon\frac{n}{3},\quad \ldots,$$

et d'ajouter en tenant compte des relations (1) et (5).

223. Théorème de Smith. — Ce théorème donne l'expression du produit des indicateurs des n premiers entiers par un détermi-

nant du $n^{\text{ième}}$ ordre, dont tous les éléments, tels que D_r^s sont les plus grands codiviseurs des deux indices r et s de l'élément considéré. En d'autres termes, *si* D_r^s *désigne le plus grand codiviseur de r et de s, on a*

$$(1) \qquad \Sigma \pm D_1^1 D_2^2 \ldots D_n^n = \varphi(1).\varphi(2)\ldots\varphi(n).$$

On en déduit la valeur de $\varphi(n)$ comme le quotient de deux déterminants d'ordres n et $(n-1)$.

La démonstration de ce théorème repose sur les propriétés d'une fonction numérique à deux indices qui possède des propriétés analogues à celles de l'indicateur. Si l'on suppose

$$n = a^\alpha b^\beta c^\gamma \ldots l^\lambda,$$

on peut écrire l'expression de $\varphi(n)$ sous la forme

$$\varphi(n) = (a^\alpha - a^{\alpha-1})(b^\beta - b^{\beta-1})\ldots(l^\lambda - l^{\lambda-1}).$$

En effectuant les produits du second membre dans l'ordre habituel (n° 67), nous désignerons le développement par

$$(2) \qquad \varphi(n) = n_1 - n_2 + n_3 - n_4 + \ldots + n_{s-1} - n_s;$$

s représente le nombre des termes du développement, qui est égal à une puissance de 2, dont l'exposant renferme autant d'unités que n renferme de facteurs premiers différents. Les nombres n_1, $n_2, \ldots, n_s$ ne représentent pas tous les diviseurs de n, mais ne représentent que ceux qui sont des multiples du quotient de n par $abc\ldots l$; d'ailleurs $n_1 = n$.

Cela posé, considérons la fonction numérique $\mu(n, z)$, dans laquelle z désigne un entier positif et arbitraire, et n un entier donné,

$$(3) \qquad \mu(n, z) = D_{n_1}^z - D_{n_2}^z + D_{n_3}^z - \ldots - D_{n_s}^z;$$

nous allons démontrer que la *fonction de* SMITH possède une propriété analogue à celle du produit des indicateurs. En d'autres termes, si n est le produit de deux nombres p et q, premiers entre eux, on a, quelle que soit la valeur de l'entier z,

$$(4) \qquad \mu(p, z).\mu(q, z) = \mu(n, z).$$

En effet, on a, d'après (2),

$$\varphi(p) = p_1 - p_2 + p_3 - p_4 + \ldots,$$
$$\varphi(q) = q_1 - q_2 + q_3 - q_4 + \ldots,$$
$$\varphi(n) = n_1 - n_2 + n_3 - n_4 + \ldots;$$

mais, d'autre part, puisque $n = pq$, on a l'identité

$$\varphi(p).\varphi(q) = \varphi(n).$$

Ainsi, tout nombre n_i est le produit de deux nombres p_j et q_k, premiers entre eux, comme diviseurs de deux nombres premiers entre eux; par suite,

$$D_{n_i}^{z} = D_{p_j}^{z}.D_{q_k}^{z}.$$

Si l'on fait la somme de toutes les égalités analogues à la précédente, après avoir multiplié les deux membres de celle-ci par $(-1)^{n_i}$, on trouve précisément la formule (3).

La fonction $\mu(n, z)$ *de* Smith *est égale à l'indicateur de n ou à zéro, suivant que n est ou n'est pas un diviseur de z.* En effet, supposons d'abord que a^α soit un diviseur de z; alors, il en est de même de $a^{\alpha-1}$; on a donc, par définition,

$$\mu(a^\alpha, z) = D_{a^\alpha}^{z} - D_{a^{\alpha-1}}^{z} = a^\alpha - a^{\alpha-1} = \varphi(a^\alpha);$$

supposons maintenant $n = a^\alpha b^\beta c^\gamma \ldots l^\lambda$, il résulte, par la formule (4),

$$\mu(n, z) = \varphi(n).$$

Supposons que a^α ne soit pas un diviseur de z; on aura

$$z = a^{\alpha'} z', \qquad \text{avec} \qquad \alpha' < \alpha,$$

et, de plus, a et z' premiers entre eux. On a, par définition,

$$\mu(a^\alpha, z) = D_{a^\alpha}^{z} - D_{a^{\alpha-1}}^{z};$$

mais le plus grand codiviseur de a^α et de z est égal au plus grand codiviseur de a^α et de $a^{\alpha'}$, c'est-à-dire à $a^{\alpha'}$; il en est de même pour le plus grand codiviseur de $a^{\alpha-1}$ et de z; par suite, si a^α ne divise pas z, on a

$$\mu(a^\alpha, z) = 0.$$

Désignons par $\xi(n)$ le *déterminant de* Smith, défini par

$$\xi(n) = \Sigma \pm D_1^1 D_2^2 \ldots D_n^n;$$

ajoutons à la dernière ligne, ou de rang $n = n_1$, les lignes de rangs $n_3, n_5, \ldots, n_{s-1}$, et retranchons-en les lignes de rangs n_2, $n_4, \ldots, n_s$; la dernière ligne de $\xi(n)$ deviendra

$$\mu(n, 1),\quad \mu(n, 2),\quad \ldots,\quad \mu(n, n-1),\quad \mu(n, n),$$

ou, par suite des propriétés démontrées ci-dessus,

$$0,\quad 0,\quad \ldots,\quad 0,\quad \varphi(n).$$

On a donc la formule de récurrence

$$\xi(n) = \varphi(n) . \xi(n-1)$$

d'où l'on tire

$$\xi(n) = \varphi(n) . \varphi(n-1) . \varphi(n-2) \ldots \varphi(2) . \varphi(1).$$

C. Q. F. D.

Le déterminant de Smith a la forme suivante

$$\begin{vmatrix} 1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{1} & \ldots & 1 \\ 1 & 2 & 1 & \mathbf{2} & 1 & \mathbf{2} & \ldots & . \\ 1 & 1 & \mathbf{3} & 1 & 1 & \mathbf{3} & \ldots & . \\ 1 & \mathbf{2} & 1 & 4 & 1 & \mathbf{2} & \ldots & . \\ \mathbf{1} & 1 & 1 & 1 & 5 & \mathbf{1} & \ldots & . \\ \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{2} & \mathbf{1} & 6 & \ldots & . \\ . & . & . & . & . & . & \ldots & . \\ . & . & . & . & . & . & \ldots & . \\ 1 & . & . & . & . & . & \ldots & n \end{vmatrix}.$$

Le déterminant est symétrique; les $(p-1)$ premiers éléments de la $p^{\text{ième}}$ rangée sont respectivement égaux aux éléments de la seconde diagonale, de rang $(p-1)$, ainsi que nous l'avons figuré en caractères gras. En effet, le plus grand codiviseur de p et de q est égal au plus grand codiviseur de $(p-q)$ et de q.

Le théorème de Smith a été publié dans les *Proceedings of the London's Mathematical Society* (vol. VII, mai 1876). Il a été généralisé par M. Mansion, dans le *Messenger of Mathematics* (octobre 1877), et dans le tome II

des *Annales de la Société scientifique de Bruxelles*. Quant aux formules de M. HAMMOND, du numéro précédent, elles sont inédites et nous ont été communiquées par M. SYLVESTER.

Les déterminants de SMITH et de M. HAMMOND sont très curieux; mais nous devons faire observer qu'ils supposent, non seulement la décomposition de n en facteurs premiers, mais aussi celle de tous les entiers, jusqu'à n. C'est donc, en quelque sorte, le *Crible d'*ERATOSTHÈNE transformé en déterminant.

Exemple I. — Si tous les éléments d'un déterminant à n rangées sont égaux à 1, en exceptant ceux de la diagonale, pour lesquels a_p^p désigne le nombre des diviseurs de p, la valeur du déterminant est 1.

(MANSION.)

Exemple II. — Le déterminant à n rangées, dans lequel chaque élément est égal à 1 ou à 0, suivant que le plus grand codiviseur des deux indices est ou n'est pas un carré parfait, a pour valeur

$$(-1)^{\alpha+\beta+\gamma+\ldots+\lambda},$$

en supposant que $a^\alpha b^\beta c^\gamma \ldots l^\lambda$ représente la décomposition de la factorielle $n!$ en ses facteurs premiers. (CESARO.)

224. Formules de Legendre. — Ces formules ont pour but de *déterminer le nombre des entiers jusqu'à n, qui ne sont pas divisibles par des nombres premiers donnés*

$$a, b, c, \ldots, l,$$

inégaux deux à deux, dont le produit p surpasse n.

En désignant par λ_n le nombre cherché, et en appliquant le théorème sur les entiers approchés, à une unité près, par défaut,

$$\mathrm{E}\,\frac{n}{ab} = \mathrm{E}\,\frac{\mathrm{E}\frac{n}{a}}{b} = \mathrm{E}\,\frac{\mathrm{E}\frac{n}{b}}{a},$$

on démontre par un procédé semblable à celui qui a servi à établir la formule d'EULER (n° 216)

$$\lambda_n = n - \sum \mathrm{E}\,\frac{n}{a} + \sum \mathrm{E}\,\frac{n}{ab} - \sum \mathrm{E}\,\frac{n}{abc} + \ldots.$$

On trouve de même le nombre λ_{2n-1} des nombres impairs, jusqu'à $(2n-1)$, qui ne sont pas divisibles par des nombres premiers

inégaux deux à deux, dont le produit p surpasse $(2n-1)$. On a la formule

$$\lambda_{2n-1} = n - \sum \mathrm{E}\,\frac{n+\frac{1}{2}(a-1)}{a} + \sum \mathrm{E}\,\frac{n+\frac{1}{2}(ab-1)}{ab} \cdots.$$

Plus généralement, considérons les n premiers termes d'une progression arithmétique

$$\mathrm{A}-\mathrm{B},\quad 2\mathrm{A}-\mathrm{B},\quad 3\mathrm{A}-\mathrm{B},\quad \ldots,\quad n\mathrm{A}-\mathrm{B},$$

dans laquelle on suppose A et B premiers entre eux et $\mathrm{B} < \mathrm{A}$. Désignons par x_1 le plus petit entier positif qui rend $(\mathrm{A}x-\mathrm{B})$ divisible par le nombre premier a; désignons par x_2 le plus petit positif qui rend $(\mathrm{A}x-\mathrm{B})$ divisible par le produit ab de deux nombres premiers inégaux, et ainsi de suite. Le nombre des termes de la progression donnée, qui ne sont pas divisibles par des nombres premiers, inégaux deux à deux, dont le produit surpasse $(n\mathrm{A}-\mathrm{B})$, est donné par l'expression

$$n - \sum \mathrm{E}\,\frac{n+a-x_1}{a} + \sum \mathrm{E}\,\frac{n+ab-x_2}{ab} - \cdots.$$

On peut supposer, dans les formules précédentes, que a, b, c, ..., p, représentent l'ensemble des nombres premiers jusqu'à p, en supposant que le carré du dernier nombre premier p de cette suite ne surpasse pas le dernier terme n, $(2n-1)$, ou $(\mathrm{A}n-\mathrm{B})$, de la progression donnée. On obtient alors le nombre des termes premiers que renferme cette progression et ainsi, par exemple, la totalité des nombres premiers jusqu'à n ou jusqu'à $(2n-1)$.

Ces formules ont été obtenues par Legendre, mais elles ont été jusqu'ici de peu d'utilité, à cause de la longueur des calculs. Cependant Piarron de Mondésir est parvenu, en les transformant, à calculer le nombre des nombres premiers qui ne surpassent pas 1 000 000 (voir les *Comptes rendus de l'Association française au Congrès du Havre*, 1877). D'autre part, M. Sylvester vient de me communiquer la formule suivante :

Si l'on représente par $\mathrm{H}\frac{x}{a}$ le nombre $\frac{x}{a}$ lorsque sa partie fractionnaire est $\frac{1}{2}$, et l'*entier le plus approché* de $\frac{x}{a}$ dans les autres

cas; si l'on désigne par $a, b, c, \ldots, p$, tous les nombres premiers de 2 à p, en supposant que p^2 ne surpasse pas un nombre pair donné $2n$, la totalité des nombres premiers plus grands que n et plus petits que $2n$ est donnée par l'entier de

$$n - \sum \mathrm{H}\,\frac{n}{a} + \sum \mathrm{H}\,\frac{n}{ab} - \sum \mathrm{H}\,\frac{n}{abc} + \cdots.$$

CHAPITRE XXIII.

LES RESTES.

225. Propriétés des congruences relativement à la division. — Nous avons exposé précédemment (nos 32, 33 et 34) les propriétés fondamentales des congruences dans leurs rapports avec l'addition et la multiplication; mais ces diverses propositions ne s'appliquent à la division qu'avec certaines restrictions.

Théorème I. — *Si deux nombres sont congrus pour un module, ils sont congrus pour un diviseur quelconque du module.* En effet, la différence de ces deux nombres est, par hypothèse, un multiple du module, et, par suite, un multiple de l'un de ses diviseurs. Mais la proposition réciproque de ce théorème n'a pas lieu.

Théorème II. — *Si deux nombres sont congrus pour des modules différents, ils sont congrus, pour un module égal au plus petit comultiple des modules donnés.* En effet, si deux nombres sont congrus pour divers modules, leur différence est un multiple de ces modules et, par conséquent, un multiple de leur plus petit comultiple.

En particulier, deux nombres congrus pour différents modules, premiers entre eux deux à deux, sont congrus pour le produit des modules.

Théorème III. — *Lorsque les deux membres d'une congruence sont des multiples d'un entier premier au module, on obtient une congruence équivalente en divisant les deux membres par cet entier.* En effet, soit, pour un module quelconque m,

$$ca \equiv cb \quad (\text{mod. } m).$$

et c premier à m; par hypothèse, la différence $c(a - b)$ est divisible par m, et puisque m est premier à c, il en résulte, par le

Par conséquent, *si a et m sont premiers entre eux, la forme linéaire $(ax + b)$ engendre un système complet de restes pour le module m, lorsque l'on y remplace successivement x par les restes d'un système complet.*

227. Nombres associés à 1 pour le module m. — En particulier, si l'on considère les restes par m des $(m - 1)$ termes de la suite

$$a,\quad 2a,\quad 3a,\quad \ldots,\quad (m-1)a,$$

dans laquelle on suppose a et m premiers entre eux et $a < m$, il existe toujours un terme $a\alpha$ de cette progression, et un seul, qui donne 1 pour reste. On dit alors que les nombres a et α sont *associés* à 1 pour ce module [1]; d'ailleurs, si a et m ne sont pas premiers entre eux, le terme $a\alpha$ ne peut donner 1 pour reste.

Pour un module premier p, un entier, autre que 1, ou $(p-1)$, ne peut être égal à son associé. En effet, lorsque l'on suppose $a = \alpha$, on en déduit que $(a^2 - 1)$, ou que le produit

$$(a+1)(a-1)$$

est divisible par p; par suite, p étant premier divise $(a + 1)$ ou $(a - 1)$ et l'on en tire $a = 1$, ou $a = (p - 1)$.

Lorsque le module est composé, l'étude des nombres égaux à leurs associés est importante en Arithmétique, utile dans les applications industrielles. Elle sera l'objet de développements ultérieurs, aux Chapitres sur les Résidus quadratiques et sur les Lois arithmétiques du Tissage.

La notion des nombres associés ramène l'étude des diviseurs de la forme $(x^n \pm y^n)$ à ceux de la forme $(z^n \pm 1)$. En effet, en supprimant d'abord les codiviseurs de x et de y, on peut supposer x et y premiers entre eux. Par conséquent, si un nombre quelconque d divise $(x^n \pm y^n)$, ce nombre est premier à x et à y; désignons par β l'associé de y pour le module d, nous aurons

$$\beta^n(x^n \pm y^n) \equiv (\beta x)^n \pm 1 \pmod{d},$$

[1] GAUSS, *Disq. Arith.*, n° 77.

et, si l'on désigne par z le reste de la division de βx par d, on voit que d divise $(z^n \pm 1)$.

Plus généralement, *tout diviseur d'une forme homogène $f(x, y)$, dans laquelle on suppose x et y premiers entre eux, est un diviseur de la forme $f(z, 1)$*. D'ailleurs, cette propriété s'applique aux formes homogènes contenant un nombre quelconque de variables.

Enfin, nous observerons que, pour un module m, au lieu d'associer à 1 les nombres premiers au module, on peut les associer à l'un quelconque D des $\varphi(m)$ nombres entiers, premiers et inférieurs au module. Par conséquent, si a et D sont deux nombres inférieurs et premiers au module m, on peut toujours trouver un nombre α, et un seul, compris entre o et m, tel que l'on ait

$$a\alpha \equiv \mathrm{D} \quad (\mathrm{mod.}\, m);$$

cette remarque sera utilisée plus tard.

228. Restes du triangle arithmétique. — Il est utile de connaître, dans un très grand nombre de questions, les restes des termes du triangle arithmétique par un module premier [1]. On a d'abord la proposition suivante : *Si p est un nombre premier, les coefficients de la puissance du binôme d'exposant p sont divisibles par p, en exceptant les coefficients extrêmes qui sont égaux à* 1. En effet, soit le nombre entier, on a

$$\mathrm{C}_p^q = \frac{p(p-1)\ldots(p-q+1)}{1.2.3\ldots q};$$

lorsque q est compris entre o et p, le module p est premier à 1, 2, 3, ..., q, et, par suite, à $q!$. Donc cette factorielle divise le produit $(p-1)(p-2)\ldots(p-q+1)$, et l'on a

$$\mathrm{C}_p^q \equiv 0 \quad (\mathrm{mod.}\, p).$$

(1) Dans son *Mémoire sur la théorie des nombres*, présenté à l'Académie des Sciences le 31 mai 1830, CAUCHY indique différents procédés pour simplifier le calcul des restes du triangle arithmétique (p. 233-244). — Voir une addition à la fin du volume.

Restes des Termes du triangle arithmétique de Pascal *pour le module* 5.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	1	.	.	**1**																						
1	1	1	.																							
2	1	2	1	.	.																					
3	1	3	3	1	.																					
4	1	4	6	4	1																					
5	1	.	.	**1**		1	.		**1**																	
6	1	1	.			1	1	.																		
7	1	2	1	.	.	1	2	1	.	.																
8	1	3	3	1	.	1	3	3	1	.																
9	1	4	6	4	1	1	4	6	4	1																
10	1	.	.	**1**		1	.	.	**2**		1	.	.	**1**												
11	1	1	.			1	1	1			1	1	1													
12	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.											
13	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.											
14	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1											
15	1	.	.	**1**		1	.	.	**3**		1	.	.	**3**		1	.	.	**1**							
16	1	1	.			1	1	.			1	1	.			1	1	.								
17	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.						
18	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.						
19	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1						
20	1	.	.	**1**		1	.	.	**4**		1	.	.	**6**		1	.		**4**		1	.		**1**		
21	1	1	.			1	1	.			1	1	.			1	1	.			1	1	.			
22	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.	1	2	1	.	.	
23	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.	1	3	3	1	.	
24	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1	1	4	6	4	1	
25	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1

Prenons, par exemple, $p = 5$, et construisons le triangle arithmétique, en supprimant les multiples de 5; nous avons alors le Tableau précédent, dans lequel chaque rectangle représente les cinq premières lignes du triangle arithmétique; les zéros sont remplacés par des points, et les termes de chacun des rectangles sont multipliés respectivement par des nombres, représentés en gros caractères dans chaque coin supérieur à droite; ces nombres reproduisent eux-mêmes les cinq premières lignes du triangle de Pascal. On a donc, en général, pour le nombre premier p,

$$C_m^n \equiv C_{m_1}^{n_1} C_{\mu_1}^{\nu_1} \quad (\text{mod.}\, p),$$

en désignant par m_1 et n_1 les quotients approchés par défaut dans la division de m et de n par p, et par μ_1 et ν_1 les restes positifs. On a, de même, en désignant par m_2 et n_2 les quotients approchés de m_1 et de n_1 et par μ_2 et ν_2 les restes par p,

$$C_{m_1}^{n_1} \equiv C_{m_2}^{n_2} C_{\mu_2}^{\nu_2} \quad (\text{mod.}\, p).$$

En remplaçant successivement $C_{m_1}^{n_1}$, $C_{m_2}^{n_2}$, ..., on a donc

$$C_m^n \equiv C_{\mu_1}^{\nu_1} C_{\mu_2}^{\nu_2} C_{\mu_3}^{\nu_3} \cdots \quad (\text{mod.}\, p).$$

Par cette formule, on ramène le problème de trouver le reste de C_m^n par p, à celui de trouver les restes de nombres C_μ^ν, dans lesquels μ et ν sont plus petits que p. D'ailleurs le reste est nul, si l'un des nombres ν est plus grand que le μ correspondant. En particulier, si m et n sont divisibles par p, on a

$$C_m^n \equiv C_{m_1}^{n_1} \quad (\text{mod.}\, p);$$

si m est divisible par p, et si n ne l'est pas,

$$C_m^n \equiv 0 \quad (\text{mod.}\, p).$$

Lorsque l'on a remplacé C_m^n et C_μ^ν, où μ et ν désignent des nombres plus petits que p, on peut encore remplacer μ par son reste minimum suivant le module p. En effet, si l'on écrit la $p^{\text{ième}}$ ligne du triangle arithmétique en supprimant les multiples de p,

$$1, \quad 0, \quad 0, \quad 0, \quad \ldots, \quad 0, \quad 0, \quad 1,$$

et si l'on forme le triangle arithmétique de bas en haut (n° 12), on trouve facilement, en supposant que l'indice supérieur de C soit plus petit que l'indice inférieur,

$$C_{p-1}^{n} \equiv (-1)^n \qquad (\text{mod.}\, p),$$

$$C_{p-2}^{n} \equiv (-1)^n \frac{n-1}{1} \qquad (\text{mod.}\, p),$$

$$C_{p-3}^{n} \equiv (-1)^n \frac{(n-1)(n+2)}{2} \qquad (\text{mod.}\, p).$$

Ainsi on a les théorèmes suivants :

Si p est un nombre premier, les coefficients de la puissance du binôme d'exposant $(p-1)$ *sont alternativement congrus à* $+1$ *et à* -1 *pour le module p.*

Les coefficients de la puissance d'exposant $(p-2)$ *sont respectivement congrus à la suite alternée des* $(p-1)$ *premiers nombres entiers.*

Les coefficients de la puissance d'exposant $(p-3)$ *sont respectivement congrus à la suite alternée des* $(p-2)$ *premiers nombres triangulaires.*

Et ainsi de suite.

Exemple I. — Pour que tous les termes d'une ligne du triangle arithmétique soient impairs, il faut et il suffit que le rang de cette ligne soit une puissance de 2, diminuée de 1.

Exemple II. — Trouver la condition pour que le produit des termes d'une ligne du triangle arithmétique ne soit pas divisible par un nombre premier p, et calculer le reste du produit par p.

Exemple III. — Trouver les restes des termes d'une ligne du triangle arithmétique par un module égal à la puissance d'un nombre premier.

229. Théorème de Fermat. — Nous avons vu (n° 27) que si a désigne un entier quelconque, la différence $(a^5 - a)$ est divisible par 10 et, par conséquent, par 5. En général, on a le théorème suivant :

Si l'on désigne par p un nombre premier quelconque, et par a un nombre entier quelconque, la différence $(a^p - a)$ *est un multiple de p.*

En d'autres termes, dans un système de numération dont la base est un nombre premier p, les puissances d'exposants 1 et p d'un nombre quelconque, sont terminées par le même chiffre.

Pour démontrer ce théorème, on remarque d'abord que la différence $(a^p - a)$ est un multiple de p, quelle que soit la valeur du nombre premier p, pour $a = 0$ et pour $a = 1$. Il suffit donc de faire voir que, en admettant la proposition pour une valeur donnée a, elle a lieu encore lorsque l'on augmente a de 1. Mais on a, d'après le numéro précédent,

$$(a+1)^p \equiv a^p + 1 \pmod{p},$$

et, par suite, en retranchant $(a+1)$ des deux membres,

$$(a+1)^p - (a+1) \equiv a^p - a \pmod{p}.$$

Puisque le second membre est divisible par p, il en est de même du premier. Donc la proposition est générale et subsiste pour les valeurs négatives de a.

On énonce encore sous une forme différente le théorème précédent :

Si p désigne un nombre premier et a un nombre quelconque non divisible par p, la différence $(a^{p-1} - 1)$ *est un multiple de p.*

En effet, on a

$$a^p - a = a(a^{p-1} - 1);$$

donc p divise le second membre; mais p et a sont premiers entre eux, puisque p est un nombre premier qui ne divise pas a; donc p divise l'autre facteur du second membre. Ainsi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ce théorème, remarquable par son élégance et par son utilité, est le théorème fondamental de l'Arithmétique supérieure. Il a été énoncé par FERMAT qui n'en a pas donné de démonstration, bien qu'il ait assuré qu'il l'avait trouvée. EULER en a publié la première démonstration conforme à la précédente.

La démonstration d'EULER a été publiée sous le titre *Theoremata Arith. nova meth. demonstr.* dans les *Comm. nov. Acad. Petrop.*

(t. VIII, p. 74). Antérieurement, EULER n'était pas encore arrivé au résultat (*Comm. Petrop.*, t. VI, p. 106). Dans la fameuse discussion entre MAUPERTUIS et KÖNIG sur le principe de la moindre action, celui-ci assura qu'il avait entre les mains un manuscrit autographe de LEIBNIZ qui contenait une démonstration de ce théorème, conforme à celle d'EULER (*Appel au public*, p. 106). « Quoique nous ne voulions pas refuser de croire à ce témoignage, dit GAUSS (*Disq. Arithm.*, n° 50), il est sûr cependant que LEIBNIZ n'a jamais publié sa démonstration. » Voir l'*Histoire de l'Académie de Berlin* (1750, p. 130), et la démonstration de LAMBERT dans les *Acta Eruditorum* (1769, p. 109). Pour nous, il nous paraît impossible d'admettre que cette démonstration, si simple et si naturelle, trouvée par LEIBNIZ, EULER et LAMBERT n'ait pu être imaginée par FERMAT qui a non seulement énoncé le théorème, mais en a déduit de nombreux corollaires dont l'exactitude a été démontrée.

On peut donner du théorème de FERMAT une autre démonstration qui diffère peu de la précédente, mais qui conduit à une formule utile pour d'autres recherches. En tenant compte des congruences du triangle arithmétique, on a, pour p premier,

$$(a+b)^p \equiv a^p + b^p \pmod{p};$$

en remplaçant b par $(b+c)$,

$$(a+b+c)^p \equiv a^p + (b+c)^p \pmod{p},$$

ou, en développant $(b+c)^p$,

$$(a+b+c)^p \equiv a^p + b^p + c^p \pmod{p},$$

et ainsi de suite, de telle sorte qu'on a la formule [1]

$$(a+b+c+\ldots+l)^p \equiv a^p + b^p + c^p + \ldots + l^p \pmod{p}.$$

En supposant $a = b = c = \ldots = l = 1$, et ces unités en nombre quelconque, on retrouve le théorème en question.

Exemple I. — Vérifier la congruence

$$2^{37.73-1} \equiv 1 \pmod{37.73}.$$

On a d'abord

$$2^{36} \equiv 1 \pmod{37},$$
$$2^{9} \equiv 1 \pmod{73},$$

[1] On peut encore obtenir cette formule, ainsi que l'a fait GAUSS (*Disq. Arithm.*, n° 51), par le développement de la puissance d'exposant p du polynôme

$$(a+b+c+\ldots+l).$$

et, par suite,

$$2^{36} \equiv 1 \quad (\text{mod}. 73);$$

mais les modules 37 et 73 sont premiers entre eux, on a donc

$$2^{36} \equiv 1 \quad (\text{mod}. 37.73);$$

et, en élevant à la puissance d'exposant 75 les deux membres de la congruence précédente, il vient, puisque $37.73 = 36.75 + 1$,

$$2^{37.73-1} \equiv 1 \quad (\text{mod}. 37.73).$$

Cette congruence montre que le théorème de **Fermat** peut s'appliquer à des nombres composés et que, par conséquent, il n'a pas de réciproque. Nous montrerons cependant que l'on peut, avec certaines restrictions, donner un énoncé qui constitue la proposition réciproque du théorème de **Fermat** (n° **240**).

Il arrive, mais dans des cas assez rares, que $(a^{p-1} - 1)$ soit divisible, non seulement par p, mais aussi par p^2; ainsi $(3^{10} - 1)$ est divisible par 11^2. Pour $a = 10$, le nombre $(10^2 - 1)$ est non seulement divisible par 3, mais aussi par 3^2. On a encore vérifié que, pour $a = 10$ et p premier inférieur à 1000, il n'existe qu'une seule autre valeur du nombre premier p, telle que l'on ait

$$10^{p-1} \equiv 1 \quad (\text{mod}. p^2);$$

cette valeur exceptionnelle est $p = 487 = 2.3^5 + 1$. Ceci montre qu'il ne faut pas toujours se hâter de conclure par induction dans l'étude des propriétés des nombres.

Exemple II. — Démontrer que le quotient de $(2^{p-1} - 1)$ par le nombre premier p n'est un carré que pour $p = 2, 3, 7$.

En effet, pour p impair et égal à $(2q + 1)$, on déduit

$$(2^q - 1)(2^q + 1) = px^2;$$

par suite, puisque les facteurs du premier membre sont premiers entre eux, l'un d'eux est un carré impair et l'autre le produit par p d'un carré impair; donc

$$2^q = y^2 \pm 1;$$

mais, en prenant le signe +, l'équation possible pour $q = 1$ est impossible pour $q > 1$, puisque le second membre est $\equiv 2 \,(\text{mod}. 8)$. D'autre part, en prenant le signe —, on a

$$2^q = (y + 1)(y - 1),$$

et, par suite,

$$y \pm 1 = 2.$$

Exemple III. — Existe-t-il un nombre premier p, tel que $(2^{p-1} - 1)$ soit divisible par p^2?

Exemple IV. — Si a est un entier non divisible par le nombre premier p, on a la congruence des indicateurs

$$\varphi(a^p) \equiv \varphi(a) \qquad (\text{mod.}\, p),$$

analogue à celle de FERMAT.

Exemple V. — *Restes des nombres parfaits pairs.* — Nous avons vu que tous les nombres parfaits pairs sont choisis parmi les nombres (n° 208)

$$e_p = 2^{p-1}(2^p - 1),$$

dans lesquels le second facteur est premier; par conséquent l'exposant p est aussi premier.

On voit que : *Tout nombre parfait pair, autre que* 6, *est divisible par* 4, *et que tout nombre parfait pair autre que* 6 *et* 28 *est divisible par* 16.

Tout nombre premier p plus grand que 3 est de l'une des formes $(6q+1)$ ou $(6q+5)$; d'autre part, on a

$$2^3 \equiv -1 \qquad (\text{mod.}\ 9),$$
$$2^{6q} \equiv +1 \qquad (\text{mod.}\ 9);$$

par suite, pour

$$p = 6q+1, \qquad e_p \equiv 1(2-1) \equiv 1 \qquad (\text{mod.}\ 9),$$
$$p = 6q+5, \qquad e_p \equiv 1(2^2-1) \equiv 1 \qquad (\text{mod.}\ 9);$$

donc : *Tout nombre parfait pair, autre que* 6, *est un multiple de* 9 *augmenté de* 1.

Il en résulte que si l'on fait le total des chiffres d'un nombre parfait autre que 6, puis la somme des chiffres du total, et ainsi de suite, on arrive à 10 ou à un multiple de 10 (KRAFT, *Novi Comm. Petrop.*, 1734).

On a de même, pour le module 7, la congruence $2^3 \equiv 1$; par suite, pour

$$p = 6q+1, \qquad e_p \equiv 1(2-1) \equiv +1 \qquad (\text{mod.}\ 7),$$
$$p = 6q+5, \qquad e_p \equiv 2(2^2-1) \equiv -1 \qquad (\text{mod.}\ 7);$$

donc : *Tout nombre parfait pair, autre que* 28, *est un multiple de* 7 *augmenté ou diminué de* 1.

De même, pour le module 13, la congruence $2^6 \equiv -1$, appliquée aux nombres des formes

$$p = 12q + 1,\ 5,\ 7,\ 11$$

donne cette proposition : *Tout nombre parfait pair, autre que* 6, *est un multiple de* 13 *augmenté de* 1, 2, 3 *ou* 8.

On a encore $2^9 \equiv -1$ (mod. 19); en appliquant ce résultat aux nombres d'EUCLIDE pour les nombres des formes

$$p = 18q + 1,\ 5,\ 7,\ 11,\ 13,\ 17,$$

il vient : *Tout nombre parfait pair, autre que* 6 *et* 28, *est un multiple de* 19 *augmenté de* 1, 2, 3, 7, 10 *ou* 15.

On a enfin $2^{10} \equiv -1$ (mod. 25); en appliquant ce résultat aux nombres d'EUCLIDE pour les exposants p des formes

$$p = 20q + 1, 3, 7, 9, 11, 13, 17, 19,$$

on trouve : *Tout nombre parfait pair, autre que* 496, *est un multiple de* 25 *augmenté de* 1, 3, 6, 11 *ou* 16.

En combinant ce résultat avec le premier, il en résulte que : *Tout nombre parfait pair, autre que* 6 *ou* 496, *est terminé par l'ensemble des deux chiffres* 16, 28, 36, 56 *ou* 76.

On trouverait de même les restes des nombres parfaits pairs pour les modules 11, 23, 29, 31, 37, 41, 43 et 1000 (*Mathesis,* t. IX).

Exemple VI. — Sur les nombres parfaits impairs. — On a le théorème suivant énoncé par LIONNET (*Nouvelles Annales de Mathématiques*, 1879; p. 306) :

S'il existe des nombres parfaits impairs, ils sont donnés par la formule

$$(1) \qquad n = a^{4\alpha+1} P^2,$$

dans laquelle a désigne un nombre premier de forme $(4q+1)$ *et* P *un nombre impair, plus grand que* 1, *non divisible par a.*

En effet, en conservant les notations du n° 213, on aurait

$$2n = ABC\ldots,$$

et puisque n est impair, un seul des nombres A, B, C, ... est double d'un impair, A par exemple, et les autres B, C, ... sont impairs. Mais, puisque $a, b, c, \ldots$ sont impairs, on a

$$A \equiv \alpha + 1, \quad B \equiv \beta + 1, \quad C \equiv \gamma + 1, \quad \ldots \quad (\text{mod. } 2);$$

il faut donc que $\beta, \gamma, \ldots$ soient pairs et que $(\alpha + 1)$ soit le double d'un nombre impair; donc, si l'on remplace α par $(4\alpha + 1)$ et $\beta, \gamma, \ldots$, par $2\beta, 2\gamma, \ldots$, on a

$$(2) \qquad n = a^{4\alpha+1} b^{2\beta} c^{2\gamma} \ldots;$$

d'autre part, a étant impair, on ne peut faire que les deux hypothèses $a \equiv +1$ et $a \equiv -1$ (mod. 4); par suite, a est un nombre premier de forme $(4q+1)$.

D'ailleurs les nombres $\beta, \gamma, \ldots$ ne peuvent être tous nuls en même temps; car on aurait, dans le cas contraire,

$$2a^{\alpha} = \frac{a^{\alpha+1} - 1}{a - 1} \quad \text{ou} \quad a^{\alpha}(2 - a) = 1,$$

ce qui donnerait $a = 1$ et $n = 1$. D'où résulte encore cette proposition : *Il n'existe aucun nombre parfait impair de forme* $(4q + 3)$.

Exemple VII. — S'il existe un nombre impair et parfait, ce nombre est divisible par quatre facteurs premiers inégaux deux à deux.

Exemple VIII. — Soit n_1 la somme des facteurs premiers de n, en y comprenant l'unité; soit n_2 la somme des facteurs premiers de n_1, et ainsi de suite. Démontrer que le résultat final sera toujours égal à 3 ou à 6.
(OLTRAMARE.)

230. Théorème de Fermat généralisé. — EULER a donné une généralisation du théorème de FERMAT, sous la forme suivante :

Si a et n sont premiers entre eux, la puissance de a, dont l'exposant est égal à l'indicateur de n, est congrue à +1 pour le module n.

En effet, on a pour p premier, non diviseur de a,

$$a^{p-1} = 1 + hp:$$

si l'on élève à la puissance d'exposant p les deux membres de l'égalité précédente, en tenant compte des restes du triangle arithmétique pour le module p (n° 228), il vient

$$a^{(p-1)p} = 1 + h'p^2;$$

si nous élevons encore les deux membres à la puissance d'exposant p, il vient

$$a^{(p-1)p^2} = 1 + h''p^3,$$

et ainsi de suite. Donc, en posant $P = p^\pi$, on a

$$a^{\varphi(P)} \equiv 1 \quad (\text{mod. } P).$$

Ainsi le théorème est démontré pour une puissance quelconque d'un nombre premier. Cela posé, désignons par P, Q, R, ... des puissances de nombres premiers inégaux deux à deux, par n le produit PQR ..., et par a un nombre premier à n et, par conséquent, premier à chacun des facteurs de n; on aura

$$\begin{array}{ll} a^{\varphi(P)} \equiv 1, & (\text{mod. } P), \\ a^{\varphi(Q)} \equiv 1, & (\text{mod. } Q), \\ a^{\varphi(R)} \equiv 1, & (\text{mod. } R), \\ \dots\dots & \dots\dots; \end{array}$$

mais, par la formule de l'indicateur d'un produit (n° **219**),

$$\varphi(n) = \varphi(P)\varphi(Q)\varphi(R), \quad \ldots;$$

par suite, en élevant les deux membres des congruences précédentes à une certaine puissance, de manière à obtenir l'exposant $\varphi(n)$, on trouve

$$a^{\varphi(n)} \equiv 1 \quad (\text{mod. } P),$$
$$a^{\varphi(n)} \equiv 1 \quad (\text{mod. } Q),$$
$$a^{\varphi(n)} \equiv 1 \quad (\text{mod. } R),$$
$$\ldots\ldots \quad \ldots\ldots;$$

puisque les modules P, Q, R, ..., sont premiers entre eux deux à deux (n° **225**), on déduit

$$a^{\varphi(n)} \equiv 1 \quad (\text{mod. } n).$$

C'est dans cette congruence que consiste le théorème de FERMAT généralisé par EULER (¹).

231. Deuxième démonstration des théorèmes de Fermat et d'Euler. — Désignons par p un nombre premier, et par a un nombre non divisible par p, et par conséquent premier à p; les restes des termes consécutifs de la progression arithmétique

$$a, \quad 2a, \quad 3a, \quad \ldots, \quad (p-1)a$$

par p sont inégaux deux à deux et reproduisent dans un certain ordre tous les nombres entiers

$$1, \quad 2, \quad 3, \quad \ldots, \quad (p-1).$$

Soit, pour le module p,

$$a \equiv r_1,$$
$$2a \equiv r_2,$$
$$3a \equiv r_3,$$
$$\ldots\ldots\ldots,$$
$$(p-1)a \equiv r_{p-1};$$

en multipliant membre à membre

$$(p-1)!\,a^{p-1} \equiv (p-1)!, \quad (\text{mod. } p).$$

(¹) EULER, *Theoremata arithm. nova meth. demonstr.;* (*Comm. nov. Ac. Petrop.*, t. VIII, p. 74).

En divisant les deux membres de la congruence par la factorielle $(p-1)!$, nombre premier à p, on retrouve le premier énoncé du théorème de FERMAT,

$$a^{p-1} \equiv 1 \quad (\text{mod. } p).$$

Pour retrouver le second énoncé de ce théorème, il suffit de remarquer que si a n'est pas premier au nombre premier p, il divise p; on a donc, pour toute valeur entière de a,

$$a^p \equiv a \quad (\text{mod. } p).$$

Pour démontrer le théorème d'EULER, désignons par a et n deux entiers premiers entre eux; remplaçons successivement x dans la forme ax par les N nombres

$$a_1, a_2, a_3, \ldots, a_N$$

d'un système complet de restes premiers au module n, de telle sorte que l'on a $N = \varphi(n)$. Soit donc

$$(1) \qquad \left.\begin{array}{l} aa_1 \equiv b_1 \\ aa_2 \equiv b_2 \\ aa_3 \equiv b_3 \\ \ldots\ldots\ldots \\ aa_N \equiv b_N \end{array}\right\} (\text{mod. } n)$$

les nombres $b_1, b_2, \ldots, b_N$ forment un système complet de restes (n° 226). On a donc,

$$a_1 a_2 a_3 \ldots a_N \equiv b_1 b_2 b_3 \ldots b_N \quad (\text{mod. } n),$$

attendu que chaque facteur du premier membre est congru à un facteur du second. Si l'on multiplie membre à membre les congruences (1), on obtient

$$a^N a_1 a_2 \ldots a_N \equiv a_1 a_2 \ldots a_N \quad (\text{mod. } n),$$

et en divisant les deux membres de cette congruence par le second membre, premier au module, on a

$$a^{\varphi(n)} \equiv 1 \quad (\text{mod. } n).$$

232. Perfectionnements du théorème d'Euler. — Si nous désignons

par P, Q, R, ... les puissances des nombres premiers contenues dans un nombre n, nous avons les congruences

$$\begin{aligned} a^{\varphi(\mathrm{P})} &\equiv 1 \pmod{\mathrm{P}}, \\ a^{\varphi(\mathrm{Q})} &\equiv 1 \pmod{\mathrm{Q}}, \\ a^{\varphi(\mathrm{R})} &\equiv 1 \pmod{\mathrm{R}}, \\ \ldots\ldots & \quad \ldots\ldots\ldots \end{aligned}$$

Cependant, si l'un des nombres P, Q, R, ... est pair et égal à 2^α, avec $\alpha > 2$, on doit remplacer l'indicateur par sa moitié, puisque l'on a, pour tout nombre impair a,

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Cela posé, avec cette restriction que l'on remplace $\varphi(2^\alpha)$ par $\frac{1}{2}\varphi(2^\alpha)$, lorsque l'on a $\alpha > 2$, désignons par $\psi(n)$ le plus petit comultiple des indicateurs de P, Q, R, ...; nous aurons

$$\begin{aligned} a^{\psi(n)} &\equiv 1 \pmod{\mathrm{P}}, \\ a^{\psi(n)} &\equiv 1 \pmod{\mathrm{Q}}, \\ a^{\psi(n)} &\equiv 1 \pmod{\mathrm{R}}, \\ \ldots\ldots & \quad \ldots\ldots\ldots; \end{aligned}$$

et, puisque les modules sont premiers entre eux, deux à deux,

$$a^{\psi(n)} \equiv 1 \pmod{n}.$$

Nous donnerons au plus petit comultiple $\psi(n)$ des indicateurs de P, Q, R, ... le nom d'*indicateur réduit de n*. Pour n égal à 2, à 4, à une puissance quelconque d'un nombre premier impair, ou au double d'une puissance d'un nombre premier impair, l'indicateur réduit $\psi(n)$ est égal à $\varphi(n)$; mais, dans tous les autres cas, l'indicateur réduit est une partie aliquote de l'indicateur.

Par conséquent : *Si a et n sont premiers entre eux, la puissance de a, dont l'exposant est égal à l'indicateur réduit de n, est congrue à $+1$ pour le module n.*

On peut donner au théorème d'Euler un second énoncé qui s'applique à tous les entiers x, premiers ou non, au module n. Désignons par λ le plus grand des exposants des divers facteurs premiers contenus dans n, et par p l'un quelconque des facteurs

On démontre de la même façon que les restes de $\Delta^2 x^q$ par 4 sont tous égaux à 2 si q est pair, et ceux des différences d'ordre supérieur sont nuls. En particulier, les restes de Δx^q par le module 2 sont tous égaux à 1.

2° Dans l'application de la seconde méthode, nous prendrons pour module un nombre p impair et premier, et nous calculerons les restes de $\Delta^{p-1} x^{p-1}$, pour des valeurs entières consécutives de x.

On a, par une formule du calcul des différences

$$(1) \qquad \Delta^{p-1} x^{p-1} = (p-1)!;$$

ainsi les différences d'ordre $(p-1)$ sont constantes, quelle que soit la valeur de x. Pour déterminer cette valeur constante, reprenons la formule symbolique (n° 76)

$$\Delta^{p-1} u_0 \doteq (u-1)^{p-1},$$

il vient, pour $x = 0$

$$\Delta^{p-1} 0^{p-1} = (p-1)^{p-1} - C_{p-1}^{1}(p-2)^{p-1} + \ldots - C_{p-1}^{p-2} 1^{p-1} + 0^{p-1};$$

en appliquant le théorème de Fermat aux puissances du second membre, on a

$$\Delta^{p-1} x^{p-1} \equiv (1-1)^{p-1} - 1 \pmod{p},$$

ou, plus simplement,

$$\Delta^{p-1} x^{p-1} \equiv -1 \pmod{p};$$

en comparant ce résultat avec celui de l'identité (1), on a

$$(p-1)! \equiv -1 \pmod{p}.$$

Ainsi, pour tout nombre premier p, le produit de tous les entiers inférieurs à p, augmenté de 1, est divisible par p; c'est l'énoncé du théorème de Wilson, sur lequel nous reviendrons plus loin.

3° Considérons, plus généralement, les restes de $\Delta^{n-1} x^q$ par un module quelconque n. Par le dernier théorème du numéro précédent, on peut supposer q égal au plus à $(n-1)$; si l'on suppose n composé et > 4, on peut supposer $q < n-1$, et alors les restes sont nuls; mais si n est égal à un nombre premier p, et si l'on fait

$$q = h(p-1) + r,$$

on aura

$$x^q \equiv x^r \quad \text{et} \quad \Delta^{p-1} x^q \equiv \Delta^{p-1} x^r \pmod{p};$$

lorsque $r < p - 1$, la différence $\Delta^{p-1} x^q$ est nulle ; lorsque $r = p - 1$, on a comme au 2°, $\Delta^{p-1} x^q \equiv -1$; mais alors $(p-1)$ est un diviseur de q.

En résumé, *les restes de $\Delta^{n-1} x^q$ par n sont constants.* Ils sont égaux :

A -1, si n est un nombre premier tel que $(n-1)$ divise q ;

A $+2$, si n est égal à 4 et si q est impair ;

A 0, dans tous les autres cas.

234. Théorème de Clausen et de Staudt (1). — *On a, pour les nombres de Bernoulli, l'expression*

$$B_q = A_q - \frac{1}{2} - \frac{1}{b} - \frac{1}{c} - \ldots - \frac{1}{l},$$

dans laquelle on désigne par A_q un nombre entier et par 2, b, c, ..., l tous les nombres premiers qui surpassent de 1 tous les diviseurs de q.

En effet, nous avons trouvé pour B_q l'expression

$$B_q = -\frac{\Delta_1}{2} + \frac{\Delta_2}{3} - \frac{\Delta_3}{4} + \ldots + (-1)^q \frac{\Delta_q}{q+1}.$$

D'après les résultats précédents, les fractions du second membre se réduisent à des entiers, lorsque le dénominateur n est un nombre composé > 4, ou lorsque n est un nombre premier tel que $(n-1)$ ne soit pas diviseur de q. D'ailleurs, pour $n = 4$, la fraction $-\frac{1}{4}\Delta_3$ se réduit à un nombre entier, puisque l'on doit supposer q pair, attendu que les nombres de Bernoulli d'indice impair sont nuls, à l'exception de B_1. Il ne reste donc que les fractions dont le dénominateur est un nombre premier p qui surpasse de 1 tout diviseur de q ; dans ce cas, la fraction se réduit à un entier diminué de $\frac{1}{p}$. C. Q. F. D.

(1) Staudt, *Journal de Crelle* (t. XXI, p. 72). — Clausen, *Astronomische Nachrichten*. La démonstration du texte est plus simple que celles que nous avons publiées dans *Mathesis* (t. III, p. 25, et t. XI, p. 9) et dans le *Bulletin de la Société mathématique*.

On a, pour les premières valeurs de q,

$$A_0 = A_2 = A_4 = \ldots = A_{12} = -1, \qquad A_{2q+1} = 0,$$

$$\begin{array}{ll}
A_{14} = -2, & A_{24} = -86576, \\
A_{16} = -6, & A_{26} = -1425518, \\
A_{18} = -56, & A_{28} = -27298230, \\
A_{20} = -528, & A_{30} = -601580875, \\
A_{22} = -6193, & A_{32} = -15116315766.
\end{array}$$

Exemple I. — Si q est un nombre premier et $(2q-1)$ un nombre composé, le dénominateur de B_{2q} est 6.

Exemple II. — Si q et q' sont premiers entre eux, le dénominateur de $B_{2qq'}$ est divisible par le sixième du produit des dénominateurs de B_{2q} et de $B_{2q'}$ (voir une démonstration de M. RADICKE dans la *Nouvelle Correspondance mathématique*, t. VI, p. 69; 1880).

235. Théorèmes de Genocchi et d'Adams. — On déduit immédiatement du théorème énoncé dans le numéro précédent que *le produit*

$$(1) \qquad x(x^q - 1)B_q,$$

est entier, quel que soit l'entier x. Il suffit de démontrer que le coefficient du nombre B_q est divisible par tous les nombres qui surpassent de 1 tous les diviseurs de q. Or, pour p premier, on a

$$x(x^{p-1} - 1) \equiv 0 \pmod{p},$$

et, puisque $(p-1)$ divise q, on a

$$x(x^q - 1) \equiv 0 \pmod{p}.$$

En particulier, pour $x = 2$, *les nombres*

$$G_q = 2(1 - 2^q)B_q,$$

sont entiers. Ce théorème a été énoncé, mais démontré autrement, par GENOCCHI [1]. Nous en avons donné une autre démonstration au n° 142.

---

[1] GENOCCHI, *Sur les nombres de Bernoulli* (*Ann. de Tortolini*, 1852). Voir aussi *Nouv. Ann. de Math.*, 1877; p. 157.

M. ADAMS a calculé, par l'emploi du théorème de STAUDT, la Table des nombres de BERNOULLI jusqu'à B_{124} [1]. Pour vérifier ces calculs vraiment laborieux, puisque les numérateurs des douze derniers de ces nombres ont plus de 80 chiffres, l'auteur a énoncé et démontré le théorème suivant : *Si $p > 3$ est un nombre premier, le numérateur de B_{2p} est divisible par p.* De plus, il a observé que, *si p désigne un nombre impair et premier, diviseur de q, et non diviseur du dénominateur de B_{2q}, le numérateur de B_{2q} est divisible par p;* mais l'auteur ajoute qu'il n'a pas obtenu la démonstration de cette proposition, bien qu'il ne doute pas de son exactitude. Nous allons donner la démonstration du premier théorème, en réservant pour le second volume la démonstration du second théorème de M. ADAMS.

On a, par ce qui précède,

$$B_{2p} = \frac{G_{2p}}{2(1-2^p)(1+2^p)}.$$

D'ailleurs G_{2p} est entier, impair, et divisible par p, comme cela résulte d'une formule du n° 142; mais p ne peut diviser le dénominateur de la fraction précédente; donc p restera en facteur dans le numérateur de B_{2p}.

Exemple I. — Démontrer, pour p premier, la formule

$$n G_{n+p-1} \equiv (n-1) G_n \quad (\text{mod. } p).$$

236. Restes des nombres d'Euler. — Nous avons vu (n° 145) que les nombres d'EULER sont donnés par la formule récurrente

$$(E+1)^n + (E-1)^n \simeq 0.$$

Les nombres d'indice impair sont nuls, et les nombres d'indice pair sont entiers et impairs ; de plus, SCHERK [2] a démontré que les nombres d'indice pair sont terminés alternativement par les chiffres 1 et 5. Ces propriétés sont des cas particuliers des suivantes. En tenant compte des résultats obtenus pour les restes des termes du

---

[1] ADAMS, *Journal de Borchardt*, t. LXXXV, p. 269.

[2] *Journal de Crelle*, t. LXXIX, p. 67. — Pour plus de développements, voir nos articles dans le *Bulletin de la Société mathématique*.

triangle arithmétique pour un module premier (n° **228**), la formule précédente donne, en supposant $n = (p-1)$ et p premier,

$$E_{p-1} + E_{p-3} + E_{p-5} + \ldots + E_2 + E_0 \equiv 0 \qquad (\text{mod. } p);$$

on a donc cette proposition : *Si p est un nombre premier, la somme des nombres eulériens dont l'indice ne surpasse pas p est divisible par p.*

De même, on obtient les formules

$$\left.\begin{array}{l} E_{p+1} \equiv E_2 \\ E_{p+3} \equiv E_4 \\ E_{p+5} \equiv E_6 \\ \ldots\ldots\ldots \end{array}\right\} (\text{mod. } p),$$

et, en général, pour un nombre quelconque h, entier et positif,

$$E_{2n+h(p-1)} \equiv E_{2n} \qquad (\text{mod. } p).$$

Par suite : *Les restes des nombres eulériens, suivant un module premier p, se reproduisent périodiquement dans le même ordre, dans une période de* $(p-1)$ *restes.*

Nous avons étendu ces propriétés aux nombres eulériens des divers ordres, et à un grand nombre de coefficients différentiels. Nous appelons *nombres eulériens d'ordre* α, en supposant α entier et positif, les nombres entiers donnés par la relation symbolique

$$E_{\alpha,n} \triangleq [E' + E'' + E''' + \ldots + E^{(\alpha)}]^n,$$

dans laquelle on remplace, après le développement, les exposants de E', E'', ... par des indices. On démontre, comme ci-dessus, la relation

$$E_{\alpha,n+h(p-1)} \equiv E_{\alpha,n} \qquad (\text{mod. } p).$$

237. Restes des sommes des puissances semblables des entiers inférieurs à un nombre premier. — Désignons par S_n la somme des puissances d'exposant n des $(p-1)$ premiers nombres entiers, et par p un nombre premier.

Nous allons démontrer le théorème suivant : *La somme* S_n *est congrue à* -1 *ou à* 0, *pour le module p, suivant que n est ou n'est pas multiple de* $(p-1)$. En effet, si n est un multiple de

$(p-1)$, tous les termes de S_n sont congrus à 1, d'après le théorème de FERMAT, et, puisque la somme a $(p-1)$ termes, on aura

$$S_n \equiv -1 \qquad (\text{mod. } p).$$

Pour le second cas, où n n'est pas multiple de $(p-1)$, considérons la formule symbolique [n° **132**, formule (3)]

$$x^n - 1 \triangleq (S+1)^n - S^n;$$

si l'on y remplace x par p et S_0 par $(p-1)$, il vient, en supprimant les multiples de p,

$$C_n^1 S_{n-1} + C_n^2 S_{n-2} + \ldots + C_n^{n-1} S_1 \equiv 0 \qquad (\text{mod. } p).$$

Mais S_1 est divisible par p; par suite, en faisant $n=2$, on en déduit que S_2 est aussi divisible par p, puis S_3, S_4, ..., jusqu'à S_{p-2}.

On arrive aux mêmes résultats, en partant de la formule symbolique (n° **134**)

$$(n+1) S_n \triangleq (p+B)^{n+1} - B^{n+1};$$

on multiplie les deux membres par $n!$, et l'on sait que $n!\,B_n$ est un nombre entier.

238. Théorème de Wilson. — Nous avons vu (n°s **227** et **233**) que, pour un module p, impair et premier, les entiers inférieurs à p peuvent être associés deux à deux, de telle sorte que leur produit soit congru à 1 pour le module p. D'autre part, à l'exception des nombres 1 et $(p-1)$, aucun autre nombre ne peut être égal à son associé; ainsi les nombres

$$2,\quad 3,\quad 4,\quad \ldots,\quad (p-2)$$

s'associent deux à deux, leur produit est congru à $+1$ pour le module p; on a donc

$$(p-2)! \equiv +1 \qquad (\text{mod. } p).$$

En multipliant les deux membres par $(p-1)$, il vient

$$(p-1)! + 1 \equiv 0 \qquad (\text{mod. } p).$$

En d'autres termes, *le produit de tous les entiers inférieurs à un nombre premier p, augmenté de 1, est divisible par p* (¹).

Lorsque p n'est pas premier, mais > 4, *le produit des* $(p-2)$ *premiers nombres est divisible par p.* — En effet :

1° Si p n'est pas un carré, il est décomposable en un produit de deux facteurs inégaux contenus dans la suite des $(p-2)$ premiers nombres;

2° Si $p>4$ est égal à un carré n^2, la factorielle $(p-2)!$ contient les deux facteurs n^2 et $2n^2$; elle est donc divisible par p;

3° Si $p=4$, le produit des deux ou des trois premiers nombres est congru à 2 pour le module 4.

Le théorème de Wilson donne une condition nécessaire et suffisante pour qu'un nombre soit premier; mais il est inapplicable en pratique. Cependant, on simplifie le calcul en remplaçant les nombres de la seconde partie de la factorielle $(p-1)!$ par leurs compléments à p; on en déduit d'ailleurs quelques conséquences. Nous considérerons deux cas, suivant que le reste du nombre impair et premier p par 4 est 1 ou 3.

1° Si l'on suppose $p=4q+3$, on a

$$[(2q+1)!]^2-1\equiv 0 \pmod{p}.$$

Par conséquent, *pour que* $p=4q+3$ *soit un nombre premier, il faut et il suffit que le reste de la division de la factorielle* $(2q+1)!$ *par p soit* ± 1. Cependant, on peut déterminer dans quels cas le reste est $+1$, et dans quels cas il est égal à -1 (²).

2° Si l'on suppose $p=4q+1$, on a

$$[(2q)!]^2+1\equiv 0 \pmod{p}.$$

Par conséquent, *pour que* $p=4q+1$ *soit un nombre pre-*

(¹) Waring a énoncé ce théorème, sans démonstration, dans les *Meditationes algebraicæ,* en l'attribuant à Wilson, l'un de ses élèves. Waring avoue que la démonstration lui paraît d'autant plus difficile qu'il n'y a point de notation pour désigner spécialement les nombres premiers. La démonstration du texte est due à Gauss (*Disq. Arithm.*, n° 77); celle du n° 233, qui repose sur le calcul des différences, est une simplification de celle de Lagrange.

(²) « Il n'est pas facile de dire *a priori* lequel de ces deux nombres $(2q+1)!\pm 1$ est multiple de p. » (Lebesgue, *Introduction à la Théorie des Nombres*, p. 82). Nous montrerons plus loin qu'il faut prendre $+1$ ou -1, suivant que le nombre des non-résidus quadratiques de p, compris entre 0 et $\frac{1}{2}p$, est pair ou impair.

mier, il faut et il suffit que le reste par p du carré de la factorielle $(2q)!$ *soit égal à* -1. De cette proposition, il résulte encore que tout nombre premier de la forme $(4q+1)$ divise (x^2+1), c'est-à-dire une somme de deux carrés premiers entre eux.

239. **Restes de la progression géométrique.** — Soit n un module quelconque; désignons par ψ l'indicateur réduit et par a un nombre premier à n; nous allons étudier les restes des termes de la progression géométrique

$$1, \quad a, \quad a^2, \quad a^3, \quad \ldots,$$

de raison a, divisés par n. D'abord, on ne trouve aucun reste nul, puisque a et n sont premiers entre eux; d'ailleurs, tous les restes sont premiers à n, et puisque leur nombre ne peut surpasser l'indicateur $\psi(n)$ de n, on trouvera deux puissances différentes, a^s et a^{s+t}, donnant le même reste. On a donc

$$a^s a^t \equiv a^s \pmod{n},$$

et puisque a^s est premier au module, il vient

$$a^t \equiv 1 \pmod{n}.$$

Il existe donc une puissance de a qui donne 1 pour reste, ce qui résulte d'ailleurs du théorème d'Euler. Mais, parmi toutes les puissances de a qui donnent 1 pour reste, la plus importante à considérer est celle du plus petit exposant, en ne tenant pas compte de l'exposant zéro. Soit donc g le plus petit exposant tel que l'on ait

$$a^g \equiv 1 \pmod{n};$$

on dit alors que *a appartient à l'exposant minimum g pour le module n*; mais, pour la rapidité du langage, nous dirons que g est le *gaussien* de a pour le module n.

Les g premiers restes des puissances,

$$(1) \qquad 1, \quad a, \quad a^2, \quad \ldots, \quad a^{g-1},$$

sont tous différents, car si l'on avait

$$a^{s+t} \equiv a^s \pmod{n},$$

on en déduirait $a^t \equiv 1$, et g ne serait pas le plus petit exposant

qui correspondrait au reste 1. L'ensemble des restes de la suite (1), tous distincts, et en nombre g s'appelle la *période* du nombre a pour le module n. Les restes suivants, des termes de la progression géométrique, reproduisent indéfiniment la même période; on a, en effet,

$$a^g \equiv 1, \quad a^{g+1} \equiv a, \quad a^{g+2} \equiv a^2, \quad \ldots \quad (\text{mod. } n).$$

En général, si l'on désigne par q le quotient et par r le reste de la division de s par le gaussien g, on a

$$s = qg + r \quad \text{et} \quad a^s \equiv a^{qg} a^r \equiv a^r \quad (\text{mod. } n).$$

Ainsi deux puissances a^s et a^t sont congrues ou non pour le module n, suivant que leurs exposants s et t sont congrus ou non, pour le module g, gaussien de n. En particulier, si l'on a $a^s \equiv 1$ le reste de s par g est égal à 0; il en résulte que les exposants des puissances de a qui donnent 1 pour reste sont tous les multiples du gaussien. Mais, par le théorème d'Euler perfectionné, on a

$$a^{\psi(n)} \equiv 1 \quad (\text{mod. } n).$$

Par conséquent, *le gaussien de a pour le module n est un diviseur de l'indicateur réduit de n, et les exposants des puissances de a qui, divisées par n, donnent pour reste* 1, *sont tous les multiples du gaussien.*

Exemple I. — Pour un même module, le gaussien du produit $abc\ldots$ de nombres premiers au module est un diviseur du plus petit comultiple des gaussiens des facteurs.

Exemple II. — Si l'on désigne par $x\,a\,b\,c\,d, \ldots$ et A, B, C, D, ... des nombres entiers, et si l'on pose

$$\varphi(x) = \mathrm{A}a^x + \mathrm{B}b^x + \mathrm{C}c^x + \mathrm{D}d^x + \ldots,$$

on a, pour tout nombre premier p, quelle que soit la valeur du nombre h, entier et positif, la congruence

$$\varphi[x + h(p-1)] \equiv \varphi(x) \quad (\text{mod. } p).$$

Exemple III. — Soit g le gaussien de a pour le module premier p, démontrer que la somme des puissances $q^{\text{ièmes}}$ des termes de la période est congrue à 0 ou à g, suivant le module q, selon que l'exposant q est ou n'est pas multiple du gaussien g.

240. Réciproque du théorème de Fermat. — Soit un nombre impair quelconque n; nous avons vu que la différence $n - \varphi(n)$ est toujours positive, et n'est égale à 1 que pour n premier; d'autre part, l'indicateur réduit $\psi(n)$ n'est jamais supérieur à l'indicateur $\varphi(n)$. Par conséquent, lorsque le gaussien de a pour le module n est égal à $(n - 1)$, il en résulte que n est nécessairement un nombre premier: mais, si l'on a la congruence

$$a^{n-1} \equiv 1 \pmod{n},$$

les exposants des puissances de a congrues à l'unité, qui seraient inférieurs à $(n - 1)$, ne pourraient être que des multiples d'un certain diviseur de $(n - 1)$; on a donc la proposition suivante, que l'on doit considérer comme la réciproque du théorème de Fermat : *Si $a^x - 1$ est divisible par n, pour x égal à $(n - 1)$, et n'est pas divisible par n pour x égal à une partie aliquote de $(n - 1)$, le nombre n est premier.*

Nous avons énoncé pour la première fois ce théorème en 1876, au Congrès de l'Association française pour l'Avancement des Sciences, à Clermont-Ferrand, dans une Note intitulée: *Sur la recherche des grands nombres premiers*. Nous en donnerons, dans le second volume, un grand nombre de corollaires.

Exemple I. — Soit

$$a = 3, \qquad n = 65537 = 2^{16} + 1;$$

les diviseurs de $(n - 1)$ sont

$$1, \ 2, \ 2^2, \ 2^3, \ 2^4, \ 2^5, \ \ldots, \ 2^{16}.$$

Si l'on calcule les restes par n des puissances de 3 dont les exposants sont égaux aux termes de la suite précédente, en observant que chaque reste s'obtient en divisant par n le carré du reste précédent, on trouve

$$3, \ 9, \ 81, \ 6561, -11088, \ \ldots, \ +1,$$

et, puisqu'il n'y a aucun reste égal à $+1$ avant le dernier de la suite, on en conclut que $2^{16} + 1 = 65537$ est un nombre premier.

CHAPITRE XXIV.

LES FRACTIONS CONTINUES.

241. Fractions continues. — Pour donner une valeur approchée d'un nombre fractionnaire positif $x = (a:b)$, on prend le quotient q_0 le plus approché par défaut et l'on pose, en se reportant aux notations du n° **189**,

$$x = q_0 + \frac{1}{x_1}, \quad \text{avec} \quad x_1 = \frac{b}{r_1};$$

q_0 est nul pour $x < 1$, mais entier et positif pour $x > 1$. En général, x_1 est un nombre fractionnaire > 1; pour évaluer ce nombre, on prend encore le quotient q_1 le plus approché par défaut, et l'on pose

$$x_1 = q_1 + \frac{1}{x_2}, \quad \text{avec} \quad x_2 = \frac{r_1}{r_2};$$

de même, si l'on désigne par q_2 le plus grand entier contenu dans x_2, et si l'on pose

$$x_2 = q_2 + \frac{1}{x_3}, \quad \text{avec} \quad x_3 = \frac{r_2}{r_3};$$

on obtient par le remplacement de x_1 et x_2 dans l'expression de x

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{x_2}}, \qquad x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{x_3}}},$$

et ainsi de suite. Mais le calcul des quotients $q_0, q_1, q_2, q^3, \ldots,$ revient à l'opération de la recherche du plus grand codiviseur de a et de b; on a, en général,

$$x_{p-1} = q_{p-1} + \frac{1}{x_p}, \quad \text{avec} \quad x_p = \frac{r_{p-1}}{r_p}.$$

L'opération se trouve nécessairement limitée après un nombre fini de divisions; on a ainsi

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}}.$$

On dit alors que l'on a développé x en fraction continue; les entiers $q_0, q_1, q_2, \ldots, q_n$ sont positifs et s'appellent *quotients incomplets;* le premier peut être nul, mais tous les autres sont au moins égaux à 1, et le dernier à 2, car si l'on avait $q_n = 1$, on pourrait remplacer le quotient précédent q_{n-1} par $(q_{n-1} + 1)$. On dit encore que les fractions

$$\frac{1}{q_1}, \quad \frac{1}{q_2}, \quad \ldots, \quad \frac{1}{q_n}$$

sont les *fractions intégrantes;* les nombres $x_1, x_2, \ldots, x_n$ sont les *quotients complets.* Les fractions continues successives formées de 1, 2, 3, ..., n fractions intégrantes sont appelées *fractions convergentes;* mises sous la forme de fractions ordinaires, ce sont les *réduites successives.* On a d'ailleurs ce théorème :

Tout nombre positif, entier ou fractionnaire, est, d'une seule manière, égal à une fraction continue.

Considérons trois nombres quelconques positifs x, y, z, rangés par ordre de grandeur croissante. Si le premier quotient incomplet de x et de z est le même, ce sera aussi le quotient incomplet de y; on aura

$$x = q_0 + \frac{1}{x_1}, \qquad y = q_0 + \frac{1}{y_1}, \qquad z = q_0 + \frac{1}{z_1},$$

et les quotients complets x_1, y_1, z_1 seront rangés par ordre de grandeur décroissante. De même, si x_1 et z_1 ont le même quotient incomplet q_1, ce sera celui de y_1, et l'on aura

$$x_1 = q_1 + \frac{1}{x_2}, \qquad y_1 = q_1 + \frac{1}{y_2}, \qquad z_1 = q_1 + \frac{1}{z_2};$$

les quotients complets x_2, y_2, z_2 seront rangés par ordre de grandeur croissante, et ainsi de suite; d'où résulte ce second théorème :

Lorsque trois nombres positifs, rangés par ordre de grandeur, sont développés en fractions continues, les premiers quotients incomplets qui sont communs aux deux fractions extrêmes sont aussi les premiers quotients incomplets du nombre intermédiaire, et les quotients qui complètent les trois fractions sont aussi rangés par ordre de grandeur.

D'ailleurs, ces quotients complets sont rangés dans le même ordre de grandeur que les nombres donnés (x, y, z), ou dans l'ordre contraire, suivant que le nombre des quotients incomplets communs est pair ou impair.

242. Calcul des réduites. — Les premières réduites de x sont

$$\frac{q_0}{1},\quad \frac{q_0 q_1 + 1}{q_1},\quad \frac{q_0 q_1 q_2 + q_2 + q_0}{q_1 q_2 + 1},\quad \ldots;$$

nous les désignerons respectivement par

$$\frac{f_0}{g_0},\quad \frac{f_1}{g_1},\quad \frac{f_2}{g_2},\quad \ldots.$$

Chacune des premières réduites peut se former en multipliant les deux termes de la précédente par le quotient incomplet auquel on s'arrête, et en ajoutant respectivement les deux produits obtenus aux deux termes de la fraction antéprécédente. Ainsi l'on a, pour les premières valeurs de p,

$$(1)\qquad \begin{cases} f_p = q_p f_{p-1} + f_{p-2}, \\ g_p = q_p g_{p-1} + g_{p-2}. \end{cases}$$

On démontre que ces formules sont générales et s'appliquent pour toutes les valeurs de p, en remplaçant

$$q_p \quad\text{par}\quad q_p + \frac{1}{q_{p+1}}.$$

Par conséquent, *les numérateurs et les dénominateurs des réduites successives sont des entiers positifs et croissants;* nous démontrons plus loin que les réduites calculées par ces formules sont des fractions irréductibles. D'autre part, si l'on remplace le

quotient incomplet q_{p+1} par le quotient complet x_{p+1}, on a, pour x, l'expression

$$(2)\qquad x = \frac{x_{p+1} f_p + f_{p-1}}{x_{p+1} g_p + g_{p-1}}.$$

Pour les théories qui vont suivre, il est utile d'indiquer une forme spéciale du développement d'un nombre en fraction continue. Puisque le dernier quotient q_n (complet et incomplet) est plus grand que 1, on peut le remplacer par

$$(q_n - 1) + \frac{1}{1},$$

et augmenter ainsi le nombre des fractions intégrantes de la fraction continue. La valeur de la fraction continue reste la même, mais on a introduit une fraction convergente intermédiaire

$$\frac{f_n - f_{n-1}}{g_n - g_{n-1}};$$

cependant, on doit observer que cette transformation ne peut s'effectuer que pour le dernier quotient, complet et incomplet, et qu'on ne peut l'appliquer aux autres quotients incomplets. Par suite : *Le nombre des fractions intégrantes d'une fraction continue est, à volonté, pair ou impair.*

243. Différence de deux réduites. — La différence Δ de deux réduites consécutives a pour expression

$$\Delta_p = \frac{f_{p+1}}{g_{p+1}} - \frac{f_p}{g_p} = \frac{q_{p+1} f_p + f_{p-1}}{q_{p+1} g_p + g_{p-1}} - \frac{f_p}{g_p},$$

d'où l'on tire

$$\begin{vmatrix} f_p & g_p \\ f_{p+1} & g_{p+1} \end{vmatrix} = - \begin{vmatrix} f_{p-1} & g_{p-1} \\ f_p & g_p \end{vmatrix};$$

par conséquent, les différences Δ_p et Δ_{p-1} ont des numérateurs égaux et de signes contraires; mais, pour les deux premières réduites, ce numérateur est 1 ; on a donc

$$(1)\qquad f_{p-1} g_p - f_p g_{p-1} = (-1)^p.$$

En d'autres termes, *la différence de deux réduites consécu-*

tives d'une fraction continue a pour numérateur 1, et pour dénominateur le produit des dénominateurs des deux réduites.

On a les égalités

$$\frac{f_1}{g_1}-\frac{f_0}{g_0}=\frac{1}{g_0 g_1},$$

$$\frac{f_2}{g_2}-\frac{f_1}{g_1}=-\frac{1}{g_1 g_2},$$

$$\cdots\quad\cdots\quad\cdots$$

$$\frac{f_p}{g_p}-\frac{f_{p-1}}{g_{p-1}}=-\frac{(-1)^p}{g_{p-1} g_p};$$

en ajoutant, on trouve

$$\frac{f_p}{g_p}-\frac{f_0}{g_0}=\frac{1}{g_0 g_1}-\frac{1}{g_1 g_2}+\cdots-\frac{(-1)^p}{g_{p-1} g_p}.$$

Au lieu de commencer à la première réduite, on peut commencer à une réduite quelconque; on a donc cette proposition :

La différence de deux réduites quelconques d'une fraction continue est égale à la somme alternée de fractions décroissantes dont les numérateurs sont égaux à 1.

244. Propriétés des réduites. — De la formule (1) du numéro précédent, on déduit que tout codiviseur de f_p et g_p, ou de f_p et f_{p-1}, ou encore de g_p et de g_{p-1} divise ± 1. Par conséquent, on a cette proposition :

Les réduites d'une fraction continue sont irréductibles : les numérateurs, ainsi que les dénominateurs de deux réduites consécutives, sont premiers entre eux.

Plus généralement, considérons une réduite $(f_p : g_p)$ de rang quelconque, et désignons par x_p le quotient complet correspondant; nous avons, par la formule (2) du n° 242, en remplaçant x_{p+1} par $(r_p : r_{p+1})$,

$$x=\frac{r_p f_p+r_{p-1} f_{p-1}}{r_p g_p+r_{p+1} g_{p-1}};$$

mais les deux termes de la valeur de x sont deux fonctions linéaires et homogènes de r_{p+1} et de r_p, dont le déterminant des coefficients est égal à ± 1. Donc (n° 195) :

Si l'on remplace un quotient incomplet d'une réduite par un quotient complet égal à une fraction irréductible, la réduite obtenue est irréductible.

Nous avons vu que toute réduite est égale à une somme alternée de fractions décroissantes; il en est de même de la dernière, égale à x; d'où il résulte que *les réduites de rang impair sont croissantes et ne surpassent pas la dernière; les réduites de rang pair sont décroissantes et ne sont pas plus petites que la dernière.*

Si l'on figure les réduites par des longueurs portées sur une droite à partir d'un point fixe, on a une représentation géométrique très simple des propriétés précédentes. Nous pensons, avec CLAUDE BERNARD, que « *la Science doit toujours expliquer le plus obscur et le plus complexe par le plus simple et le plus clair* ». On démontre de la même façon que la somme des n premiers termes d'une série alternée dont les termes décroissent en valeur absolue jusqu'à zéro a une limite finie et déterminée, comme la série harmonique alternée

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \ldots,$$

bien que la somme des termes positifs soit infinie, ainsi que celle des termes négatifs. Par le même procédé, on démontre encore qu'une série de cette nature, que l'on appelle *semi-convergente*, a pour limite un nombre quelconque, positif ou négatif, lorsque l'on modifie convenablement l'ordre des termes, ou s'approche alternativement de deux nombres quelconques; dans ce dernier cas, la somme, quoique finie, n'a pas de limite déterminée.

245. Approximation des réduites. — La différence entre une réduite quelconque et la valeur d'une fraction continue ne surpasse pas, en valeur absolue, la différence entre cette réduite et la suivante. On a donc, en valeur absolue,

$$x - \frac{f_p}{g_p} \leqq \frac{f_{p+1}}{g_{p+1}} - \frac{f_p}{g_p};$$

mais le second membre est une fraction dont le numérateur est égal à ± 1 et le dénominateur égal au produit $g_p g_{p+1}$. Par conséquent, la différence entre une fraction continue et l'une de ses réduites ne surpasse pas, en valeur absolue, une fraction ayant pour numéra-

teur l'unité, et pour dénominateur le produit du dénominateur de la réduite par celui de la suivante. *A fortiori*, la valeur absolue de cette différence est plus petite qu'une fraction de numérateur 1 et dont le dénominateur est égal au carré du dénominateur de la réduite.

Si une fraction quelconque approche plus d'une fraction continue qu'une réduite $(f_p : g_p)$ *de rang quelconque, ses deux termes sont respectivement plus grands que ceux de la réduite considérée.*

En effet, cette fraction est nécessairement comprise entre cette réduite et la précédente; par conséquent, si nous la développons en fraction continue, ses premiers quotients incomplets seront $q_0, q_1, q_2, \ldots, q_{p-1}$; le quotient qui la termine sera $> q_p$; donc ses deux termes sont plus grands que ceux de $(f_p : g_p)$.

On peut donner plusieurs autres expressions de la différence entre une fraction continue et ses réduites. Posons

$$\delta_p = x - \frac{f_p}{g_p},$$

et remplaçons x par sa valeur tirée de la formule (2) du n° **242**, il vient

$$(1) \quad \delta_p = \frac{(-1)^p}{g_p(x_{p+1}g_p + g_{p-1})} \qquad \text{et} \qquad \delta_{p-1} = \frac{(-1)^{p+1}x_{p+1}}{g_{p-1}(x_{p+1}g_p + g_{p-1})};$$

par suite, si nous désignons par θ un nombre compris entre 0 et 1,

$$\delta_p = (-1)^p \frac{\theta}{g_p^2} \qquad \text{et} \qquad \delta_p = -\frac{g_{p-1}}{g_p x_{p+1}} \delta_{p-1}.$$

Nous allons chercher la condition nécessaire et suffisante pour qu'une fraction donnée $(f : g)$ soit l'une des réduites du développement d'un nombre x en fraction continue. Développons la fraction $(f : g)$ en fraction continue, et désignons par $(p-1)$ et p les indices des deux dernières réduites. Pour que x admette la réduite $(f_p : g_p)$, il faut et il suffit que x soit compris entre cette réduite et la précédente; par suite, si, dans la valeur de δ_p, on suppose $x_{p+1} > 1$, on aura, en valeur absolue,

$$(2) \qquad x - \frac{f_p}{g_p} < \frac{(-1)^p}{g_p(g_p + g_{p-1})}.$$

En particulier, cette inégalité est vérifiée, lorsque

$$\pm\left(x - \frac{f_p}{g_p}\right) < \frac{1}{2g_p^2}. \tag{3}$$

Réciproquement, si l'inégalité (3) est vérifiée, il en est de même de l'inégalité (2); on tire donc de la formule (1) une valeur de x_{p+1}, plus grande que 1; on aura, par conséquent,

$$x = q_0 + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_p + \cfrac{1}{x_{p+1}}}}.$$

Cependant, si le signe du second membre de l'inégalité (2) n'était pas le même que celui du premier, on augmenterait d'une fraction intégrante le développement de $(f : g)$, ainsi que nous l'avons expliqué au n° **242**.

Donc : *Pour qu'une fraction donnée $(f : g)$ soit l'une des réduites d'un nombre x développé en fraction continue, il faut et il suffit que l'on ait, en valeur absolue,*

$$x - \frac{f_p}{g_p} < \frac{1}{g_p(g_p + g_{p-1})},$$

en désignant par g_{p-1} et g_p les dénominateurs des deux dernières réduites du développement de $(f : g)$ en fraction continue.

246. Renversement des fractions continues. — Nous dirons que l'on renverse une fraction continue lorsque l'on écrit tous ses quotients incomplets dans l'ordre opposé au sens ordinaire. On a, par la loi de formation des réduites,

$$\frac{f_n}{f_{n-1}} = q_n + \frac{1}{\left(\frac{f_{n-1}}{f_{n-2}}\right)}, \qquad \frac{g_n}{g_{n-1}} = q_n + \frac{1}{\left(\frac{g_{n-1}}{g_{n-2}}\right)};$$

si l'on remplace successivement, dans les seconds membres, les fractions par d'autres équivalentes, l'application répétée de ces formules donne

$$\frac{f_n}{f_{n-1}} = q_n + \cfrac{1}{q_{n-1} + \cdots + \cfrac{1}{q_1 + \cfrac{1}{q_0}}}, \qquad \frac{g_n}{g_{n-1}} = q_n + \cfrac{1}{q_{n-1} + \cdots + \cfrac{1}{q_2 + \cfrac{1}{q_1}}}.$$

Par conséquent, *lorsque l'on renverse l'ordre des quotients incomplets d'une fraction continue, la fraction continue renversée est égale au quotient du numérateur de la dernière réduite par le numérateur de la précédente, et l'avant-dernière réduite de la fraction renversée est égale au quotient des dénominateurs des deux dernières réduites de la fraction donnée.*

247. Addition des fractions continues. — Considérons deux fractions continues

$$\frac{f_n}{g_n} = q_0 + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_n}}, \qquad \frac{f'_p}{g'_p} = s_0 + \cfrac{1}{s_1 + \cdots + \cfrac{1}{s_p}};$$

plaçons la seconde à la suite de la première en ajoutant le premier quotient incomplet s_0 de la seconde au dernier, q_n, de la première; nous formons ainsi une fraction continue

$$\frac{F_{n+p}}{G_{n+p}} = q_0 + \cfrac{1}{q_1 + \cdots + \cfrac{1}{q_n + s_0 + \cfrac{1}{s_1 + \cdots + \cfrac{1}{s_p}}}},$$

dont le nombre des fractions intégrantes est $(n+p)$, en considérant $(q_n + s_0)$ comme un seul quotient incomplet. Nous allons calculer les deux dernières réduites de cette fraction continue, au moyen des deux dernières réduites de chacune des fractions continues données. En effet, si l'on remplace

$$q_n \quad \text{par} \quad q_n + \frac{f'_p}{g'_p},$$

dans la loi de formation des réduites (n° **242**), on trouve

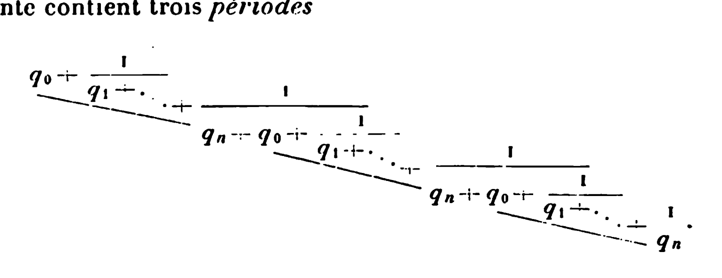
$$F_{n+p} = f_n g'_p + f_{n-1} f'_p,$$
$$G_{n+p} = g_n g'_p + g_{n-1} f'_p;$$

d'ailleurs F_{n+p} et G_{n+p} sont premiers entre eux, puisque la réduite $(f'_p : g'_p)$ est irréductible (n° **244**).

On peut supposer $s_0 = 0$; alors les formules précédentes, que nous appellerons *formules d'addition des fractions continues,*

permettent de calculer les réduites d'une fraction continue, en la décomposant en deux ou plusieurs fractions continues successives.

218. Multiplication des fractions continues. — Étant donnée une fraction continue, on peut la prolonger, autant de fois qu'on veut par des fractions continues identiques à la première et former des fractions que nous appellerons *périodiques*. Ainsi, la fraction suivante contient trois *périodes*



Nous ferons observer que nous donnons ici une certaine extension à la définition ordinaire des fractions périodiques ; pour retrouver celles que l'on considère habituellement, il suffit de supposer $q_0 = 0$. Si la fraction contient h périodes, le nombre des fractions intégrantes est égal à hn, même pour $q_0 = 0$, car nous ne considérons pas $(q_n + q_0)$ comme un quotient incomplet. Si, dans les formules d'addition, nous remplaçons n par hn, nous obtenons

$$(1) \qquad \begin{cases} F_{hn+p} = g_p F_{hn} + f_p F_{hn-1}, \\ G_{hn+p} = g_p G_{hn} + f_p G_{hn-1}, \end{cases}$$

p étant au moins égal à 1. En remplaçant p par $(h-1)n+p$, nous obtenons les formules

$$(2) \qquad \begin{cases} F_{hn+p} = f_n G_{(h-1)n+p} + f_{n-1} F_{(h-1)n+p}, \\ G_{hn+p} = g_n G_{(h-1)n+p} + g_{n-1} F_{(h-1)n+p}, \end{cases}$$

Il est préférable de se servir des formules (1) qui permettent de calculer séparément les numérateurs et les dénominateurs des réduites, de n en n [1]; mais les formules (2) sont parfois utiles. En

[1] Ces formules correspondent aux formules de Simpson dans la Trigonométrie rectiligne.

particulier, nous démontrerons que l'on a cette propriété des fractions continues périodiques

$$\frac{F_{hn}}{G_{hn-1}} = \frac{f_n}{g_{n-1}}.$$

En effet, si l'on fait $p = n$ dans la première des formules (2) et $p = (n-1)$ dans la seconde des formules (1), on obtient

$$F_{(h+1)n} = f_n G_{hn} + f_{n-1} F_{hn-1},$$
$$G_{(h+1)n-1} = g_{n-1} G_{hn} + f_{n-1} G_{hn-1};$$

d'où l'on déduit

$$g_{n-1} F_{(h+1)n} - f_n G_{(h+1)n-1} = f_{n-1}(g_{n-1} F_{hn} - f_n G_{hn-1}) = 0.$$

En particulier, nous avons les formules

$$F_{2n} = f_n(g_n + f_{n-1}), \qquad F_{2n-1} = f_{n-1}^2 + f_n g_{n-1},$$
$$G_{2n} = g_n^2 + f_n g_{n-1}, \qquad G_{2n-1} = g_{n-1}(g_n + f_{n-1}).$$

249. Fractions continues symétriques. — Nous dirons qu'une fraction continue est *symétrique*, lorsque tous ses quotients incomplets à égale distance des extrêmes sont égaux deux à deux. Soit donc la fraction continue symétrique

$$\frac{f_n}{g_n} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_2 + \cfrac{1}{q_1 + \cfrac{1}{q_0}}}}}.$$

Nous pouvons supposer $q_0 > 0$; car, s'il en était autrement, nous remplacerions la fraction donnée par son inverse. Il résulte immédiatement des résultats obtenus sur le renversement d'une fraction continue (n° 246), que $g_n = f_{n-1}$; d'ailleurs, une fraction ne peut être développée que d'une seule manière en fraction continue; par conséquent *si la fraction continue $(f_n : g_n)$ est symétrique, on a l'égalité $f_{n-1} = g_n$, et réciproquement.*

Mais la relation fondamentale

(1) $$f_n g_{n-1} - f_{n-1} g_n = (-1)^{n-1}$$

devient, dans cette hypothèse,

$$f_n g_{n-1} = g_n^2 + (-1)^{n-1};$$

donc f_n divise le second membre. Réciproquement, *si deux nombres f et g sont tels que f divise $(g^2 \pm 1)$, la fraction $(f : g)$ est développable en fraction continue symétrique.* D'abord f et g sont nécessairement premiers entre eux; convertissons $(f : g)$ en fraction continue, de telle sorte que le nombre n des fractions intégrantes soit impair ou pair, suivant que f divise $(g^2 + 1)$ ou $(g^2 - 1)$; désignons par g' le quotient correspondant, on aura

$$f_n g' = g_n^2 + (-1)^{n-1};$$

mais, si l'on désigne par f_{n-1} et g_{n-1} les deux termes de l'avant-dernière réduite, on aura la relation (1); d'où l'on tire, par différence avec la relation précédente,

$$f_n(g' - g_{n-1}) = g_n(g_n - f_{n-1}).$$

Mais f_n ou f est premier à g_n; donc f_n diviserait $(g_n - f_{n-1})$ qui est plus petit que lui; on a donc

$$g' = g_{n-1} \quad \text{et} \quad g_n = f_{n-1};$$

la dernière égalité exprime la condition de symétrie. Ainsi, lorsque f divise $(g^2 + 1)$, la fraction $(f : g)$ est une fraction continue symétrique contenant un nombre impair de fractions intégrantes, et le nombre des quotients incomplets $q_0, q_1, \ldots, q_n$ est pair; si f divise $(g^2 - 1)$, la fraction continue symétrique, égale à $(f : g)$, a un nombre impair de quotients incomplets, et n est pair.

Lorsqu'une fraction continue est symétrique, on peut calculer les deux dernières réduites, lorsque l'on connaît les deux dernières réduites qui correspondent à la première moitié de son développement. Considérons d'abord une *fraction symétrique paire*, c'est-à-dire une fraction symétrique contenant un nombre pair de quotients incomplets, et supposons $n = 2\nu + 1$; soit la fraction

$$\frac{f_n}{g_n} = q_0 + \cfrac{1}{q_1 + \ddots + \cfrac{1}{q_\nu + \cfrac{1}{q_\nu + \ddots + \cfrac{1}{q_0}}}};$$

désignons par $(f_{\nu-1} : g_{\nu-1})$ et $(f_\nu : g_\nu)$ les deux dernières réduites qui correspondent à la première moitié de la fraction continue, et par $x_{\nu+1}$ le quotient complet qui suit q_ν : nous avons trouvé

$$\frac{f_n}{g_n} = \frac{f_\nu x_{\nu+1} + f_{\nu-1}}{g_\nu x_{\nu+1} + g_{\nu-1}};$$

mais, d'autre part, $x_{\nu+1}$ est égal à $(f_\nu : f_{\nu-1})$; on a donc

$$(1) \qquad \begin{cases} f_n = f_\nu^2 + f_{\nu-1}^2, \\ g_n = f_\nu g_\nu + f_{\nu-1} g_{\nu-1}. \end{cases}$$

Puisque la fraction $(f_n : g_n)$ est symétrique, on a $f_{n-1} = g_n$, et l'on tire g_{n-1} de la relation

$$f_n g_{n-1} - f_{n-1} g_n = (-1)^n = (f_\nu g_{\nu-1} - f_{\nu-1} g_\nu)^2 :$$

on a ainsi

$$(2) \qquad \begin{cases} f_{n-1} = f_\nu g_\nu + f_{\nu-1} g_{\nu-1}, \\ g_{n-1} = g_\nu^2 + g_{\nu-1}^2. \end{cases}$$

Les formules (1) et (2) résolvent la question proposée pour $n = 2\nu + 1$, c'est-à-dire pour le cas d'une fraction continue, qui est symétrique et paire.

Si la fraction continue est symétrique et impaire, on peut l'écrire sous la forme

$$\frac{f_n}{g_n} = q_0 + \frac{1}{q_1} + \cdots + \cfrac{1}{q_{\nu-1} + \cfrac{1}{2q_\nu} + \cfrac{1}{2q_\nu + \cdots + \cfrac{1}{q_0}}},$$

en ayant le soin de remplacer la fraction intégrante médiane $\frac{1}{q_\nu}$ par $\frac{1}{2q_\nu} + \frac{1}{2q_\nu}$; on obtient alors, comme ci-dessus, en remplaçant $x_{\nu+1}$ par $(f_{\nu-1} : f_\nu)$,

$$(3) \qquad \begin{cases} f_n = 2 f_\nu f_{\nu-1}, \\ g_n = f_\nu g_{\nu-1} + f_{\nu-1} g_\nu = f_{n-1}, \\ g_{n-1} = 2 g_\nu g_{\nu-1}. \end{cases}$$

250. Sur les décompositions des nombres en carrés. — Les résultats précédents conduisent à une démonstration d'un théorème

important que nous retrouverons dans une théorie beaucoup plus générale.

Tout diviseur d'une somme de deux carrés premiers entre eux est une somme de deux carrés. En effet, si f divise une somme de deux carrés premiers entre eux, f divise (n° 227) l'expression $(g^2 + 1)$. Donc, si l'on convertit $(f : g)$ en fraction continue, on obtient une fraction symétrique paire, et l'on a

$$f = f_{2\nu+1} = f_\nu^2 + f_{\nu-1}^2.$$

Plus particulièrement, tout diviseur premier d'une somme de deux carrés est une somme de deux carrés ; mais il ne faut pas en conclure que tout nombre premier soit une somme de deux carrés. Car *aucun nombre premier* $p \equiv 3$ (*mod.* 4) *ne peut être la somme de deux carrés entiers ou fractionnaires.* En effet, si l'on avait

$$p = \frac{x^2}{x'^2} + \frac{y^2}{y'^2},$$

le nombre p diviserait une somme de deux carrés et serait une somme de deux carrés entiers, ce qui est impossible puisque cette somme est congrue à 1 ou à 2, et non à 3, pour le module 4.

Nous donnerons une autre démonstration du théorème précédent, qui repose encore sur la théorie des fractions continues, mais où l'on ne considère pas les fractions symétriques. Plus généralement, nous démontrerons, d'après une méthode due à M. HERMITE, les trois théorèmes suivants : *Tout diviseur de la forme quadratique* $(a^2 + k b^2)$ *est de la même forme, lorsque* $k = 1, 2, 3$.

En effet, ainsi que nous l'avons démontré (n° 227), il suffit de considérer les diviseurs premiers de la forme $(x^2 + k)$. Supposons donc, pour p premier, que l'on ait

$$x^2 + k \equiv 0 \pmod{p};$$

développons en fraction continue la fraction $(x : p)$, dans laquelle on peut supposer $x < \frac{1}{2}p$. Les dénominateurs des réduites vont en croissant, jusqu'à p ; désignons par g_n et g_{n+1} les deux dénominateurs consécutifs choisis de telle sorte que leurs carrés com-

prennent le nombre p. On a donc

$$\left(\frac{x}{p} - \frac{f_n}{g_n}\right)^2 < \frac{1}{(g_n g_{n+1})^2},$$

ou bien

$$(xg_n - pf_n)^2 < \frac{p^2}{g_{n+1}^2} < p,$$

et en ajoutant kg_n^2 de part et d'autre, il vient

$$(xg_n - pf_n)^2 + kg_n^2 < p + kg_n^2.$$

Mais, en développant le premier membre, on voit que celui-ci est un multiple de p. Cela posé, supposons d'abord $k = 1$: le second membre ne peut égaler $2p$; par suite, le premier membre, qui n'est pas nul et qui est un multiple de p, est précisément égal à p, et l'on a

$$(xg_n - pf_n)^2 + g_n^2 = p.$$

Supposons $k = 2$; le second membre ne peut surpasser $3p$; on a donc pour le premier membre la valeur p ou $2p$, et par suite l'une ou l'autre des représentations

$$(xg_n - pf_n)^2 + 2g_n^2 = p,$$
$$2\left(\frac{xg_n - pf_n}{2}\right)^2 + g_n^2 = p.$$

Enfin, si $k = 3$, le premier membre sera égal à p, $2p$ ou $3p$; la seconde hypothèse est impossible suivant le module 4 ; on a donc l'une ou l'autre des décompositions

$$(xg_n - pf_n)^2 + 3g_n^2 = p,$$
$$3\left(\frac{xg_n - pf_n}{3}\right)^2 + g_n^2 = p.$$

251. Multiplication des fractions continues symétriques. — Dans le cas particulier des fractions continues symétriques, les formules de multiplication se simplifient à cause de $f_{n-1} = g_n$; ainsi l'on a, en remplaçant n par hn, puisque la fraction reste symétrique (n° 249),

$$F_{2hn} = 2F_{hn}G_{hn},$$
$$G_{2hn} = 2G_{hn}^2 + (-1)^{nh-1} = F_{2hn-1},$$
$$G_{2hn-1} = 2G_{hn}G_{hn-1}.$$

Posons, d'autre part, d'après le n° 249,

$$A = \frac{f_n}{g_{n-1}} = \frac{F_{hn}}{G_{hn-1}};$$

on en déduit, par la relation fondamentale,

$$A G_{hn-1}^2 = F_{hn-1}^2 + (-1)^{hn-1}$$

et, par suite,

$$F_{2hn-1} = G_{2hn} = F_{hn-1}^2 + A G_{hn-1}^2.$$

Enfin, si l'on pose

$$X_{\mu+1} = \frac{F_\mu}{G_\mu}, \qquad Y_{\mu+1} = \frac{A G_\mu}{F_\mu},$$

on voit que les formules précédentes donnent

$$X_{2hn} = \frac{X_{hn} + Y_{hn}}{2}, \qquad \frac{2}{Y_{2hn}} = \frac{1}{X_{hn}} + \frac{1}{Y_{hn}},$$

de telle sorte que X_{2hn} et Y_{2hn} sont respectivement la moyenne arithmétique et la moyenne harmonique de X_{hn} et de Y_{hn}. Par ce procédé, on peut calculer les réduites X_μ en doublant continuellement l'indice, et obtenir ainsi $X_{2^\alpha n}$ et $Y_{2^\alpha n}$, sans calculer les fractions intermédiaires (Voir l'*Addition X*).

FRACTIONS CONTINUES GÉNÉRALISÉES.

252. Algorithme d'Euler. — Cumulants. — La notation des fractions continues est souvent incommode dans la pratique; il est préférable de se servir de l'algorithme d'EULER (¹), afin de généraliser la théorie et l'emploi des fractions continues ordinaires.

Prenons des nombres quelconques, positifs ou négatifs, entiers ou fractionnaires,

$$q_0, \quad q_1, \quad q_2, \quad \ldots, \quad q_n, \quad \ldots,$$

et formons une suite commençant par 0, 1, que nous représenterons par

$$0, \quad 1, \quad \| \quad Q_0, \quad Q_1, \quad Q_2, \quad \ldots, \quad Q_n, \quad \ldots,$$

(¹) EULER, *Solutio problematis arithmetici de inveniendo numero qui, per datos numeros divisus, relinquat data residua* (*Comm. Ac. Petrop.*, t. VII, p. 46). — *De usu novi algorithmi in problemate Pelliano solvendo* (*Nov. Comm. Petrop.*, t. XI, p. 28). — GAUSS, *Disq. Arithm.*, n° 27.

et de telle sorte que chaque terme se calcule successivement au moyen des deux précédents et du nombre q correspondant, par la loi de récurrence

$$Q_n = q_n Q_{n-1} + Q_{n-2}.$$

On effectue le calcul de la façon suivante, de gauche à droite,

		q_0	q_1	q_2	q_3	....
0	1	q_0	$q_0 q_1 + 1$	$q_0 q_1 q_2 + q_2 + q_0$	$q_3 Q_2 + Q_1$	....
		Q_0	Q_1	Q_2	Q_3	....

Si les nombres q sont entiers et positifs, Q_n désigne le numérateur de la fraction dont le développement en fraction continue donne les quotients incomplets $q_0, q_1, \ldots, q_n$; mais, dans le but de la simplification et de la généralisation, nous désignerons, avec Euler, le nombre Q_n par le symbole

$$[q_0, q_1, q_2, \ldots, q_n],$$

et nous dirons que cette expression représente le *cumulant* des $(n+1)$ éléments $q_0, q_1, q_2, \ldots, q_n$, pris dans un ordre déterminé. Avec cette notation, la loi de récurrence s'écrit

$$[q_0, q_1, \ldots, q_n] = q_n [q_0, q_1, \ldots, q_{n-1}] + [q_0, q_1, \ldots, q_{n-2}].$$

Lorsque tous les éléments sont égaux à 1, le cumulant de n éléments est égal au terme u_{n+1} de la suite de Fibonacci. Mais, plus généralement, en laissant aux éléments du cumulant des valeurs arbitraires, on aperçoit que tous ses termes sont dissemblables et ne peuvent se réduire entre eux; par suite : *Le nombre des termes du cumulant de n éléments quelconques est égal au terme u_{n+1} de la suite de* Fibonacci.

Au lieu de prendre pour valeurs initiales les nombres 0 et 1, nous pouvons prendre les nombres 1 et 0, tout en conservant la même loi de formation; nous formons ainsi des nombres R dont les premières valeurs sont

$$1, 0, \quad R_0 = 0, \quad R_1 = q_1, \quad R_2 = q_1 q_2 + 1, \quad \ldots.$$

On voit immédiatement que q_0 n'entre pas dans les valeurs de R; d'ailleurs $R_0 = 0$, $R_1 = q_1$. Par conséquent, les autres valeurs s'obtiennent avec les éléments du cumulant, en supprimant q_0. On a donc

$$R_n = [q_1, q_2, q_3, \ldots, q_n].$$

Considérons enfin une suite S ayant pour valeurs initiales $S_0 = b$ et $S_1 = a$; et calculons successivement les autres termes par la loi de formation

$$S_n = q_n S_{n-1} + S_{n-2}.$$

On aperçoit, par le calcul des premiers termes, comme pour les restes obtenus dans la recherche du plus grand codiviseur de deux nombres (n° 189), que l'on a, pour toute valeur de n, la formule

$$S_n = aX_n + bY_n,$$

dans laquelle X_n et Y_n ne contiennent ni a, ni b. Si l'on fait $a = 1$, $b = 0$, on a donc

$$X_n = [q_0, q_1, \ldots, q_n],$$

et si l'on fait $a = 0$ et $b = 1$, on a

$$Y_n = [q_1, q_2, \ldots, q_n].$$

Par conséquent, on a pour l'expression de S_{n+1}, calculée par cumulants, en prenant pour valeurs initiales S_0 et S_1, deux nombres quelconques, b et a,

$$S_n = a[q_0, q_1, \ldots, q_n] + b[q_1, q_2, \ldots, q_n].$$

D'ailleurs, en supposant arbitraires tous les éléments du cumulant, ainsi que a et b, tous les termes de S_{n+1} sont dissemblables, et leur nombre est égal au terme u_{n+2} de la suite de Fibonacci.

253. Propriétés des cumulants. — Si l'on remplace, dans la dernière formule du numéro précédent, b par 1 et a par q_0, en prenant $q_1, q_2, \ldots, q_n$ pour éléments du cumulant, on a

$$(1) \qquad [q_0, q_1, \ldots, q_n] = q_0[q_1, q_2, \ldots, q_n] + [q_2, q_3, \ldots, q_n].$$

D'ailleurs, nous avons trouvé plus haut la formule

$$(2)\quad [q_0, q_1, \ldots, q_n] = q_n[q_0, q_1, \ldots, q_{n-1}] + [q_0, q_1, \ldots, q_{n-2}].$$

Nous démontrerons d'abord cette proposition : *Si l'on change tous les signes des n éléments d'un cumulant, on multiplie celui-ci par* $(-1)^n$. En effet, cette propriété a évidemment lieu lorsque le cumulant se compose de 1, 2, 3, ... termes. Supposons qu'elle soit vérifiée pour les cumulants de $(n-2)$ et de $(n-1)$ éléments; la formule (2) nous montre qu'elle est encore vérifiée pour n éléments. Donc la propriété subsiste pour un nombre quelconque d'éléments du cumulant.

On a aussi la proposition suivante : *Quelles que soient les valeurs des éléments d'un cumulant, on a la relation*

$$(3)\quad [q_0, \ldots, q_n].[q_1, \ldots, q_{n-1}] - [q_0, \ldots, q_{n-1}][q_1, \ldots, q_n] = (-1)^{n-1}.$$

En effet, lorsque les éléments du cumulant sont des nombres entiers et positifs, la fraction continue

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_n}}},$$

est égale à la réduite (n° 242)

$$\frac{f_n}{g_n} = \frac{[q_0, q_1, \ldots, q_n]}{[q_1, q_2, \ldots, q_n]},$$

et nous avons trouvé la relation

$$f_n g_{n-1} - f_{n-1} g_n = (-1)^{n-1};$$

mais la méthode de raisonnement qui nous a permis d'établir cette formule ne suppose pas que les nombres q_n sont des entiers, et la méthode s'applique à des nombres quelconques, entiers ou fractionnaires, positifs ou négatifs. Par conséquent, la relation proposée est démontrée.

Enfin, on a encore le théorème suivant : *Un cumulant ne change pas de valeur si l'on renverse l'ordre de ses éléments.* En d'autres termes, on a l'égalité

$$(4)\quad [q_0, q_1, \ldots, q_n] = [q_n, \ldots, q_1, q_0].$$

En effet, cette propriété est vérifiée lorsque le nombre n des éléments du cumulant est égal à 1, 2 ou 3; supposons-la vérifiée pour les cumulants de $(n-2)$ et de $(n-1)$ éléments. Mais si l'on renverse, dans la formule (2), l'ordre des éléments qui sont supposés arbitraires, on a

$$[q_n, q_{n-1}, \ldots, q_0] = q_0[q_n, q_{n-1}, \ldots, q_1] + [q_n, q_{n-1}, \ldots, q_2];$$

si l'on compare cette formule avec la formule (1), on en déduit immédiatement l'exactitude du théorème énoncé.

254. Fractions continues généralisées. — On a encore considéré les fractions continues sous la forme générale

$$a_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \ddots + \cfrac{a_n}{b_n}}}},$$

dans laquelle les a et les b sont des nombres quelconques, positifs ou négatifs; on obtient pour les premières réduites

$$\begin{array}{ll} f_0 = a_0, & g_0 = 1, \\ f_1 = b_1 f_0 + a_1, & g_1 = b_1, \\ f_2 = b_2 f_1 + a_2 f_0, & g_2 = b_2 g_1 + a_2 g_0, \\ \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots, \\ \ldots\ldots\ldots\ldots, & \ldots\ldots\ldots\ldots, \\ f_n = b_n f_{n-1} + a_n f_{n-2}; & g_n = b_n g_{n-1} + a_n g_{n-2}. \end{array}$$

On pourrait ainsi tirer f_n et g_n sous forme de déterminant; mais il n'y a aucun avantage à cette transformation. On démontre, comme pour les fractions continues ordinaires, que la loi de formation des deux termes des réduites est générale. La relation fondamentale devient

$$f_p g_{p-1} - f_{p-1} g_p = (-1)^{p-1} a_1 a_2 \ldots a_p;$$

mais les réduites ne sont plus des fractions irréductibles. On a encore la série alternée

$$\frac{f_p}{g_p} - \frac{f_0}{g_0} = \frac{a_1}{g_0 g_1} - \frac{a_1 a_2}{g_1 g_2} + \frac{a_1 a_2 a_3}{g_2 g_3} - \ldots + (-1)^{p-1} \frac{a_1 a_2 \ldots a_p}{g_{p-1} g_p}.$$

Enfin, on peut remplacer ces fractions continues, au moyen de l'algorithme d'Euler, en posant

$$q_0 = a_0, \quad q_1 = \frac{b_1}{a_1}, \quad q_2 = \frac{b_2 a_1}{a_2}, \quad q_3 = \frac{b_3 a_2}{a_1 a_3}, \quad \ldots .$$

Exemple I. — Transformer en fractions continues ordinaires les fractions

$$a + \cfrac{1}{b - \cfrac{1}{c}}, \qquad a + \cfrac{1}{b - \cfrac{1}{c - \cfrac{1}{d}}}.$$

On trouve pour la première, en supposant b et $c > 1$, les quotients incomplets

$$a, \quad (b-1), \quad 1, \quad (c-1),$$

et pour la seconde, en supposant b, $(c-1)$ et $d > 1$, les quotients incomplets

$$a, \quad (c-1), \quad 1, \quad (c-2), \quad 1, \quad (d-1).$$

Exemple II. — Calculer les réduites successives de la fraction continue généralisée

$$2 - \cfrac{1}{2 - \cfrac{1}{2 - \cfrac{1}{2 - \ldots}}}$$

On trouve

$$\frac{f_0}{g_0} = \frac{2}{1}, \quad \frac{f_1}{g_1} = \frac{3}{2}, \quad \frac{f_2}{g_2} = \frac{4}{3}, \quad \ldots, \quad \frac{f_n}{g_n} = \frac{n+2}{n+1}.$$

Exemple III. — Calculer les réduites de la fraction continue

$$3 - \cfrac{2}{3 - \cfrac{2}{3 - \cfrac{2}{3 - \ldots}}}$$

On trouve

$$\frac{f_0}{g_0} = \frac{3}{1}, \quad \frac{f_1}{g_1} = \frac{7}{3}, \quad \frac{f_2}{g_2} = \frac{15}{7}, \quad \ldots, \quad \frac{f_n}{g_n} = \frac{2^{n+2}-1}{2^{n+1}-1}.$$

Remarque I. — Lorsque l'on développe un nombre fractionnaire en fraction continue ordinaire, on prend constamment le quotient incomplet par défaut; on pourrait prendre constamment le quotient incomplet par excès, et alors toutes les fractions intégrantes auraient -1 pour numérateur.

Remarque II. — On peut aussi prendre le quotient le plus approché, soit par défaut, soit par excès, et alors les fractions intégrantes auront pour numérateur, soit $+1$, soit -1, d'après la suite des calculs.

Remarque III. — Enfin, on peut encore développer un nombre fractionnaire en prenant alternativement les quotients approchés par défaut et par excès. On obtient, dans ces différents cas, des fractions continues généralisées qui peuvent être utiles dans la solution de certaines questions (¹).

255. Développement du cumulant d'éléments égaux. — On peut se proposer de développer le cumulant

$$[x, x, x, \ldots, x]_{(n)},$$

dont tous les éléments en nombre n sont égaux à x. On trouve, pour les premiers développements,

$$\begin{aligned}
[x] &= x,\\
[x, x] &= x^2 + 1,\\
[x, x, x] &= x^3 + 2x,\\
[x, x, x, x] &= x^4 + 3x^2 + 1,\\
[x, x, x, x, x] &= x^5 + 4x^3 + 3x,\\
&\ldots\ldots\ldots\ldots
\end{aligned}$$

On voit ainsi que le cumulant de n éléments égaux à x est un polynôme en x de degré n, que nous désignerons par $\varphi_n(x)$.

Il ne contient que des termes dont les exposants sont de même parité; d'ailleurs le tableau des coefficients représente le triangle arithmétique dont les lignes sont placées parallèlement à la diagonale descendante ↘. On a ainsi

$$(1) \qquad \varphi_n = x^n + C_{n-1}^1 x^{n-2} + C_{n-2}^2 x^{n-4} + C_{n-3}^3 x^{n-6} + \ldots;$$

on vérifie facilement, *a posteriori*, l'exactitude de cette formule, par la loi de formation

$$\varphi_{n+1} = x\varphi_n + \varphi_{n-1} \qquad \text{et} \qquad \varphi_0 = 1,$$

(¹) Gauss, *Disq. arith.*, n° 177.

et les égalités obtenues pour S par

$$3^{p-1},\quad 3^{p-2},\quad \ldots\quad 3^2,\quad 3,\quad 1:$$

faisons les sommes des égalités obtenues ; nous avons ainsi les formules

$$(2)\qquad \begin{cases} N_p = 2^p\,(N_0 - 1) + 1, \\ S_p = 3^p\,S_0 - \dfrac{3^p - 1}{2}\,s, \\ T_p = -3^{p-1}\,S_0 - \dfrac{3^{p-1} - 1}{2}\,s. \end{cases}$$

Plus particulièrement, si la suite initiale se compose de deux termes de somme s, on a plus simplement,

$$(3)\qquad \begin{cases} N_p = 1 + 2^p, \\ S_p = (1 + 3^p)\,\dfrac{s}{2}, \\ T_p = (1 - 3^{p-1})\,\dfrac{s}{2}. \end{cases}$$

Exemple I. — Calculer les six premières suites que l'on obtient par intercalations successives, en partant de 1 et 1.

Exemple II. — Démontrer que les deux plus grands termes de la suite obtenue après p intercalations sont égaux au terme u_{p+1}, de la suite de Fibonacci, et que leurs rangs sont donnés par l'expression

$$1 + 2^{p-2} \pm \frac{2^{p-2} - (-1)^p}{3}.$$

Exemple III. — On donne n nombres $a_0, b_0, c_0, \ldots, h_0, k_0, l_0$; on forme une première suite, $a_1, b_1, c_1, \ldots$, en remplaçant chacun d'eux par la somme de tous les autres, et ainsi consécutivement ; trouver l'expression des termes de la suite d'indice p.

En désignant par s_0 la somme des nombres donnés, l'un d'eux, c_0 par exemple, devient

$$c_p = \frac{(n-1)^p - (-1)^p}{n}\,s_0 + (-1)^p c_0.$$

(Ed. Collignon.)

257. De la médiation. — Considérons deux fractions à termes positifs

$$\frac{b}{a}\quad \text{et}\quad \frac{d}{c};$$

intercalons entre ces deux nombres une fraction ayant pour numérateur et pour dénominateur la somme des numérateurs et des dénominateurs des fractions données; nous obtenons une fraction que nous appellerons la *médiante* des deux premières. Lorsque les dénominateurs a et c sont égaux à 1, la médiante devient la moyenne arithmétique, mais il n'en est pas de même dans le cas général (nº **84**).

Ainsi, par ce procédé dit de *médiation,* dont on trouve de nombreux exemples dans les ouvrages d'Archimède et des géomètres de l'Inde, nous formons, avec les deux fractions données, la suite

(1) $$\frac{b}{a},\quad \frac{b+d}{a+c},\quad \frac{d}{c}.$$

Posons $ad - bc = \Delta$, nous trouvons pour les différences

$$\frac{d}{c}-\frac{b}{a}=\frac{\Delta}{ac},\qquad \frac{b+d}{a+c}-\frac{b}{a}=\frac{\Delta}{a(a+c)},\qquad \frac{d}{c}-\frac{b+d}{a+c}=\frac{\Delta}{c(a+c)}.$$

Par conséquent, si l'on intercale entre deux fractions quelconques, à termes positifs, leur fraction médiante, on obtient une suite (1) de trois fractions à termes positifs, rangées par ordre de grandeur, et les différences de deux fractions consécutives ont le même numérateur Δ. Intercalons les deux médiantes dans les deux intervalles de la suite (1); répétons le même procédé sur la suite obtenue et continuons de même; nous formerons ainsi des suites de fractions à termes positifs, rangées par ordre de grandeur, et la différence de deux fractions consécutives a constamment Δ pour numérateur.

Réciproquement, si l'on a trois fractions consécutives

$$\frac{b}{a},\quad \frac{y}{x},\quad \frac{d}{c},$$

telles que leurs différences successives aient un numérateur égal au numérateur de la différence des fractions extrêmes, la fraction $(y:x)$ est la médiante des deux autres. En d'autres termes, si l'on a

$$\frac{y}{x}-\frac{b}{a}=\frac{ad-bc}{ax},\qquad \frac{d}{c}-\frac{y}{x}=\frac{ad-bc}{cx},$$

[illegible]

[illegible]

[illegible]

[illegible] fractions [illegible] ou à [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

$$\frac{b}{A} = [illegible] \qquad \frac{1}{[illegible]} = \frac{[illegible]}{q_{[illegible]} - \frac{1}{q_{[illegible]} - \cdots - \frac{1}{q_{[illegible]} - \frac{d}{c}}}}$$

[illegible] $q_{[illegible]} - \frac{[illegible]}{a}$

nous allons démontrer que la fraction médiante de ces deux fractions peut s'obtenir en remplaçant les restes $(b:a)$ et $(d:c)$ par leur médiante. En effet, désignons par $(B_{n-2}:A_{n-2})$ et $(B_{n-1}:A_{n-1})$ les réduites qui correspondent aux $(n-2)$ et aux $(n-1)$ premiers quotients incomplets, nous avons

$$\frac{B}{A} = \frac{(bq_n + a)B_{n-1} + bB_{n-2}}{(bq_n + a)A_{n-1} + bA_{n-2}},$$
$$\frac{D}{C} = \frac{(dq_n + c)B_{n-1} + dB_{n-2}}{(dq_n + c)A_{n-1} + dA_{n-2}};$$

ces deux fractions ont pour médiante

$$\frac{B+D}{A+C} = \frac{\left[\overline{b+d}\,q_n + \overline{a+c}\right]B_{n-1} + \overline{b+d}\,B_{n-2}}{\left[\overline{b+d}\,q_n + \overline{a+c}\right]A_{n-1} + \overline{b+d}\,A_{n-2}}.$$

On a donc

$$\frac{B+D}{A+C} = \cfrac{1}{q_1 + \cfrac{1}{q_2 \cdots + \cfrac{1}{q_n + \cfrac{b+d}{a+c}}}};$$

d'ailleurs, si les fractions à termes positifs $(b:a)$ et $(d:c)$ ne surpassent pas 1, leur médiante est comprise entre 0 et 1.

258. Suites de Brocot. — Ces suites ont été considérées pour la première fois par Brocot, dans un intéressant opuscule sur les calculs de l'horlogerie [1]. Elles proviennent de l'intercalation successive, par voie de médiation, des deux fractions $\frac{0}{1}$ et $\frac{1}{0}$, dans l'intervalle desquelles se trouvent tous les nombres commensurables positifs. La première suite obtenue est

$$\frac{0}{1}, \quad \frac{1}{1}, \quad \frac{1}{0};$$

en nous bornant aux nombres commensurables compris entre 0 et 1, il nous suffit de conserver les deux premiers termes, puisque

---

(1) *Calcul des rouages par approximation, nouvelle méthode,* par Brocot, horloger (Paris, 1862).

les nombres commensurables inverses des premiers se trouveraient placés, dans les suites successives, à égale distance de la fraction $\frac{1}{1}$. Avec cette restriction, nous formons les suites

β_1	$\frac{0}{1}$	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	$\frac{1}{1}$;
β_2	$\frac{0}{1}$	.	.	.	.	.	.	.	$\frac{1}{2}$	.	.	.	.	.	.	.	$\frac{1}{1}$;
β_3	$\frac{0}{1}$	.	.	.	$\frac{1}{3}$	.	.	.	$\frac{1}{2}$	.	.	.	$\frac{2}{3}$	.	.	.	$\frac{1}{1}$;
β_4	$\frac{0}{1}$	.	$\frac{1}{4}$	.	$\frac{1}{3}$	.	$\frac{2}{5}$	.	$\frac{1}{2}$	.	$\frac{3}{5}$	.	$\frac{2}{3}$	.	$\frac{3}{4}$	.	$\frac{1}{1}$;
β_5	$\frac{0}{1}$	$\frac{1}{5}$	$\frac{1}{4}$	$\frac{2}{7}$	$\frac{1}{3}$	$\frac{3}{8}$	$\frac{2}{5}$	$\frac{3}{7}$	$\frac{1}{2}$	$\frac{4}{7}$	$\frac{3}{5}$	$\frac{5}{8}$	$\frac{2}{3}$	$\frac{5}{7}$	$\frac{3}{4}$	$\frac{4}{5}$	$\frac{1}{1}$;
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. ;
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. ;
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	. ;
β_p	u_p^0	u_p^1	u_p^2	u_p^3	u_p^4	.	.	.	.	.	.	.	.	.	.	.	. .

Nous allons démontrer que tout nombre commensurable à termes positifs apparaît dans l'une des suites et, par conséquent, dans toutes les suivantes; nous avons ainsi deux problèmes à résoudre : 1° Déterminer l'indice de la suite et le rang du terme de cette suite qui contient un nombre donné $(b : a)$; 2° Déterminer la valeur d'un terme de rang donné n dans une suite β_p d'indice donné.

En d'autres termes, supposons

$$u_p^n = \frac{b}{a};$$

il s'agit : 1° de calculer toutes les valeurs de n et de p qui correspondent à deux nombres donnés a et b positifs et premiers entre eux; 2° de calculer la valeur de b et celle de a qui correspondent aux valeurs données n et p de deux entiers positifs.

Nous observerons d'abord, par la loi de formation des suites, que tout terme u_p^n apparaît dans toutes les séries suivantes, et que, si p augmente d'une unité, l'indice n se trouve multiplié par 2; on a donc, pour tout entier positif α, la formule

$$u_{p+\alpha}^{2^\alpha n} = u_p^n;$$

par conséquent, pour connaître les diverses places occupées par une fraction donnée, il suffit de savoir le rang qu'elle occupe dans la suite, quand elle apparaît pour la première fois, ainsi que l'indice de cette suite.

En particulier, on a $u_1^1 = \frac{1}{1}$; la fraction $\frac{1}{1}$ apparaît donc, au rang $n = 2^{p-1}$, dans la suite d'indice p; on retrouve ainsi le nombre $N_p = (1 + 2^{p-1})$ des termes de la suite; il en résulte que l'on a toujours $n < 2^{p-1}$.

En second lieu, on voit tout de suite que le second terme u_q^1 d'une suite quelconque est $\frac{1}{q}$; par conséquent,

$$u_{q+\alpha}^{2^\alpha} = \frac{1}{q};$$

si, dans cette formule, nous remplaçons successivement α par les valeurs $1, 2, 3, \ldots (p-1)$, et q par les valeurs complémentaires $(p-1), (p-2), \ldots, 2, 1$, nous obtenons

$$u_p^1 = \frac{1}{p}, \quad u_p^2 = \frac{1}{p-1}, \quad \ldots, \quad u_p^{2^r} = \frac{1}{p-r}, \quad \ldots, \quad u_p^{2^{p-2}} = \frac{1}{2}, \quad u_p^{2^{p-1}} = \frac{1}{1}.$$

Ainsi, on peut *calculer directement la suite d'indice p, sans calculer les suites précédentes,* en écrivant les inverses des nombres entiers

$$\frac{1}{p}, \quad \frac{1}{p-1}, \quad \frac{1}{p-2}, \quad \ldots, \quad \frac{1}{3}, \quad \frac{1}{2}, \quad \frac{1}{1},$$

et en intercalant dans les intervalles successifs, par médiation, des médiantes en nombres

$$0, \quad 1, \quad 3, \quad 5, \quad \ldots. \quad (2^{p-2} - 1).$$

Pour déterminer les indices qui correspondent à la première apparition d'une fraction $(b:a)$ comprise entre 0 et 1, nous la développerons en fraction continue ordinaire. Soit donc

$$\frac{b}{a} = \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n}}}},$$

$q_1, q_2, \ldots, q_n$ désignant des entiers positifs, avec la condition $q_n > 1$.

On a donc

$$\frac{1}{q_1+1} < \frac{b}{a} < \frac{1}{q_1};$$

dans la série d'indice (q_1+1), les deux fractions qui comprennent $(b:a)$ sont consécutives, puisqu'elles ont pour rangs $n=1$ et $n=2$; par conséquent, puisque, dans la succession des suites, toutes les fractions sont rangées par ordre de grandeur croissante, cette fraction ne pourra se trouver pour la première fois que dans une suite ultérieure, et comprise entre les deux fractions extrêmes des inégalités précédentes. Cela posé, intercalons les médiantes entre les fractions continues

$$\frac{1}{q_1+\frac{1}{1}} \quad \text{et} \quad \frac{1}{q_1+\frac{0}{1}};$$

ces deux fractions ont les mêmes quotients incomplets; on peut donc faire cette opération sur les fractions $\frac{1}{1}$ et $\frac{0}{1}$; faisons q_2 intercalations successives par médiation; la fraction qui précèdera la dernière des deux précédentes $(1:q_1)$ sera

$$q_1+\frac{1}{q_2};$$

mais $(1:q_1)$ aura pour rang 2^{q_2} dans la série d'indice (q_1+q_2). Par conséquent, la fraction $\left(q_1+\frac{1}{q_2}\right)$ apparaît pour la première fois dans la série ayant pour indice (q_1+q_2) au rang $2^{q_2}+1$; elle apparaît donc dans la suivante au rang $2^{q_2+1}-2$; si l'on remplace q_2 par (q_2+1), on voit que la fraction

$$\frac{1}{q_1+\frac{1}{q_2+1}}$$

apparaît, pour la première fois, dans la série d'indice (q_1+q_2+1) au rang

$$2^{q_2+1}-1.$$

On a ensuite

$$\frac{1}{q_1+\cfrac{1}{q_2+\cfrac{0}{1}}} < \frac{b}{a} < \frac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{1}}};$$

dans la série d'indice (q_1+q_2+1), les deux fractions qui comprennent $\frac{b}{a}$ sont consécutives et ont pour rangs 1 et 2 ; en répétant le même raisonnement, on voit donc que

$$\frac{1}{q_1+\cfrac{1}{q_2+\cfrac{1}{q_3}}}$$

apparaît, pour la première fois, dans la suite β qui a pour indice $(q_1+q_2+q_3)$ et au rang $n = 2^{q_3}(2^{q_2}-1)+1$.

Il est facile de continuer l'application de la méthode précédente et d'en déduire ce théorème : *Si l'on désigne par $q_1, q_2, q_3, \ldots, q_n$ les quotients incomplets d'une fraction comprise entre* 0 *et* 1, *cette fraction apparaît, pour la première fois, sous forme irréductible, dans la suite de Brocot dont l'indice est égal à la somme des quotients incomplets, et le rang qu'elle occupe après $\frac{0}{1}$ dans cette suite a pour expression le cumulant*

$$(-1)^{n-1}[1, -2^{q_1}, +2^{q_2}, -2^{q_3}, \ldots, (-1)^{n-1}2^{q_n}].$$

La première partie de ce théorème a été énoncée par HALPHEN, mais démontrée d'une autre manière (¹). On a cette autre proposition : *La suite de Brocot d'indice p se compose de toutes les fractions irréductibles, comprises entre* 0 *et* 1, *dont la somme des quotients incomplets de leur développement en fraction continue ordinaire, ne surpasse pas l'indice p de la suite.*

Dans la suite β_p, les termes u_p^n de rang n impair représentent les fractions médiantes de la suite β_{p-1}. On a donc encore ce théorème : *Les fractions irréductibles, comprises entre* 0 *et* 1, *et dont le développement en fraction continue ordinaire donne une somme de quotients incomplets égale à p, sont en nombre* 2^{p-2}.

(¹) HALPHEN, *Sur des suites de fractions analogues à la suite de* FAREY (*Bull. Soc. math.*, t. V, p. 170; Paris, 1877).

[illegible]

[illegible]

[illegible] Suites de Farey. — [illegible]

[illegible]

[illegible] suite de *Farey* [illegible]

[illegible]

[illegible] mais en n'insérant que les fractions dont le dénominateur ne surpasse pas n; nous formons ainsi une suite incomplète de Farey, dont les propriétés fondamentales subsistent.

Toutes les fractions obtenues sont irréductibles, rangées par ordre de grandeur; chacune des fractions est égale à la médiante des deux fractions qui la comprennent; la différence de deux fractions consécutives a pour numérateur 1; deux numérateurs consécutifs, ou deux dénominateurs sont premiers entre eux.

---

(1) Ce théorème a été énoncé sous une forme un peu différente par FAREY dans le *Bulletin de la Société philomathique* (Paris, 1816), et démontré peu après par CAUCHY.

On peut d'ailleurs simplifier le calcul précédent en se bornant à l'intercalation des fractions jusqu'à $\frac{1}{2}$; on obtient les autres en retranchant les premières de 1.

Pour déterminer le nombre des termes de la suite de FAREY d'indice p, on observe que cette suite se compose de toutes les fractions irréductibles, ayant pour dénominateurs 1, 2, 3, ..., p; par conséquent, en tenant compte des fractions extrêmes $\frac{0}{1}$ et $\frac{1}{1}$, on a ce théorème :

Le nombre des fractions de la suite de Farey de rang p est égal à 1 *augmenté de la somme des indicateurs des p premiers nombres;* c'est-à-dire à

$$1 + \varphi(1) + \varphi(2) + \ldots + \varphi(p) = 1 + \int_1^p \varphi(p).$$

Si l'on retranche ce nombre du nombre des termes de la suite correspondante de BROCOT, on en déduit encore cette proposition: Les fractions irréductibles comprises entre 0 et 1, dont le dénominateur surpasse p, mais dont la somme des quotients incomplets dans le développement en fraction continue ne surpasse pas p, sont en nombre

$$2^{p-1} - \int_1^p \varphi(p)$$

Enfin, on peut encore considérer des suites analogues à celles de FAREY; on peut ainsi astreindre les numérateurs à la condition de ne pas dépasser un certain nombre donné.

Exemple I. — Former la suite de FAREY, d'indice 7. — On trouve

$$\frac{0}{1},\ \frac{1}{7},\ \frac{1}{6},\ \frac{1}{5},\ \frac{1}{4},\ \frac{2}{7},\ \frac{1}{3},\ \frac{2}{5},\ \frac{3}{7},\ \left(\frac{1}{2}\right),\ \frac{4}{7},\ \frac{3}{5},\ \ldots,\ \frac{6}{7},\ \frac{1}{1}.$$

M. SYLVESTER vient de publier plusieurs Mémoires fort intéressants sur la Partition des nombres et sur les suites de FAREY; nous y reviendrons ultérieurement.

SUR L'ÉQUATION INDÉTERMINÉE $ax + by = c$.

260. Objet de l'analyse indéterminée du premier degré. — On sait que tout système de n équations du premier degré, à n incon-

nues, donne un système unique de solutions, lorsque le déterminant Δ des coefficients n'est pas nul; mais, lorsque Δ est nul, le système est impossible ou indéterminé. Dans ce dernier cas, le nombre des équations distinctes surpasse celui des inconnues d'un entier que l'on appelle l'ordre de l'indétermination; alors on peut se proposer de ne rechercher que les valeurs entières des inconnues. Nous supposerons, dans ce qui suit, que les coefficients des inconnues et les termes connus sont tous entiers, car s'il en était autrement il suffirait de multiplier les deux membres de chaque équation par le plus petit comultiple des dénominateurs, dans les constantes réduites à leur plus simple expression. L'*Analyse indéterminée du premier degré* a donc pour objet de rechercher les solutions entières d'un système indéterminé d'équations du premier degré et à constantes entières.

Considérons une ou plusieurs équations de la forme

$$ax + by + cz + \ldots = n; \tag{1}$$

tout codiviseur des coefficients a, b, c, ... divise nécessairement n, si les inconnues sont entières. Par conséquent, pour qu'un système indéterminé soit possible, il faut d'abord que, pour chaque équation, le plus grand codiviseur des coefficients divise le terme connu; par suite, on peut supposer ces coefficients premiers entre eux. D'ailleurs, on doit observer que cette simplification ne modifie ni le signe des inconnues, ni le nombre des systèmes de solutions.

Pour abréger le langage, nous appellerons *système minimum* tout système de solutions entières pour lequel la somme des carrés des inconnues est la plus petite possible, et *système positif* tout système de solutions entières pour lequel il n'y a aucune inconnue négative.

Enfin, nous appellerons *système négatif*, tout système où l'une au moins des inconnues a une valeur négative.

261. Sur la partition des nombres. — Lorsqu'il ne s'agit que d'une seule équation, on peut supposer n non négatif, car s'il en était autrement on changerait les signes des deux membres. On peut aussi supposer positifs les coefficients des inconnues, car si un

coefficient était négatif, on changerait le signe de l'inconnue correspondante.

La recherche de tous les systèmes positifs de l'équation (1), dont les constantes sont entières et positives, constitue un problème qui rentre dans la *Partition des nombres*. Comme EULER l'a montré, ce problème revient à l'étude du développement de

$$\frac{1}{(1-\xi^a)(1-\xi^b)(1-\xi^c)\ldots},$$

ordonné suivant les exposants croissants de ξ. En effet, en supposant $\xi < 1$, on a

$$\frac{1}{1-\xi^a} = 1 + \xi^a + \xi^{2a} + \ldots + \xi^{xa} + \ldots + R_a,$$

$$\frac{1}{1-\xi^b} = 1 + \xi^b + \xi^{2b} + \ldots + \xi^{yb} + \ldots + R_b,$$

$$\frac{1}{1-\xi^c} = 1 + \xi^c + \xi^{2c} + \ldots + \xi^{zc} + \ldots + R_c,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;$$

si l'on multiplie membre à membre, on obtient une expression de la forme

$$1 + A_1\xi + A_2\xi^2 + \ldots + A_n\xi^n + \ldots + R_n,$$

dans laquelle A_n est précisément égal au nombre des systèmes positifs de l'équation (1). Les nombres a, b, c, ... étant donnés, et premiers entre eux, le coefficient A_n est une fonction de n que nous désignerons par $\varpi(n)$.

262. Résolution de l'équation à deux inconnues. — Soit l'équation

$$ax + by = c, \tag{1}$$

dans laquelle nous supposerons a et b positifs et premiers entre eux, et c non négatif. Le cas de $a = 1$, ou de $b = 1$, peut se traiter directement, mais il rentre dans la théorie générale comme celui de $c = 0$. Soit donc $a > b \geqslant 1$. On tire de l'équation donnée

$$ax - c = -by;$$

si l'on remplace x par les valeurs

$$0,\ 1,\ 2,\ \ldots\ (b-1).$$

on forme une progression arithmétique de raison a, et, puisque a et b sont premiers entre eux, on trouvera une valeur x' de x et une seule, telle que $0 \leqslant x' < b$, pour laquelle on aura

$$ax' + by' = c,$$

y' désignant un entier positif, nul ou négatif. On détermine ainsi une solution (x', y') pour laquelle x' a la plus petite valeur possible, entière et non négative.

Ainsi l'équation (1) est toujours possible et, d'une première solution quelconque (x_0, y_0), on déduit toutes les autres par les formules

$$x = x_0 + bt, \qquad y = y_0 - at,$$

t désignant un entier quelconque.

Pour trouver une première solution de l'équation (1), on développe $(a:b)$ en fraction continue; si l'on désigne par $(\alpha:\beta)$ la réduite de rang $(n-1)$, qui précède immédiatement $(a:b)$, on a

$$a\beta - b\alpha = (-1)^n;$$

d'où la solution

$$x_0 = (-1)^n c\beta, \qquad y_0 = -(-1)^n c\alpha.$$

Lorsque les coefficients a et b ne sont pas très grands, on peut encore calculer une première solution au moyen du théorème de Fermat, si b est premier, et au moyen du théorème d'Euler, si b est composé, avec les perfectionnements que nous avons indiqués au n° 232. En effet, on a, pour a et b premiers entre eux,

$$a^{\psi(b)} \equiv 1 \qquad (\text{mod. } b),$$

et si l'on pose

$$x_0 = ca^{\psi(b)-1},$$

l'expression $(c - ax_0)$ est divisible par b.

263. Systèmes minimums. — On a, pour la somme des carrés des inconnues,

$$x^2 + y^2 = (x_0 + bt)^2 + (y_0 - at)^2;$$

désignons par τ la valeur de t qui correspond au minimum; on trouve

$$\tau = \frac{ay_0 - bx_0}{a^2 + b^2},$$

et en remplaçant la solution (x_0, y_0) par celle que l'on déduit des fractions continues, on a

$$\tau = (-1)^{n-1} \frac{a\alpha + b\beta}{a^2 + b^2} c.$$

Pour que τ soit entier, il faut et il suffit que $(a^2 + b^2)$ divise c, attendu que $(a\alpha + b\beta)$ et $(aa + bb)$ sont premiers entre eux, comme fonctions linéaires de a et de b dont le déterminant des coefficients est égal à ± 1 (n° 195). On a, dans ce cas, le système minimum unique

$$x = \frac{ac}{a^2 + b^2}, \quad y = \frac{bc}{a^2 + b^2}.$$

Lorsque τ n'est pas entier, il est compris entre deux nombres entiers consécutifs t_1 et $t_2 = t_1 + 1$; si l'on désigne par ρ_1 et $-\rho_2$ les restes correspondants, on obtient les deux systèmes

$$\left\{\begin{array}{ll} (a^2 + b^2)x_1 = ac - b\rho_1, & (a^2 + b^2)x_2 = ac + b\rho_2, \\ (a^2 + b^2)y_1 = bc + a\rho_1; & (a^2 + b^2)y_2 = bc - a\rho_2. \end{array}\right.$$

Lorsque $\rho_1 = \rho_2 = \frac{1}{2}(a^2 + b^2)$, on obtient deux systèmes minimums; pour qu'il en soit ainsi, il faut et il suffit que a et b soient impairs et que c soit un multiple impair de $\frac{1}{2}(a^2 + b^2)$. Mais, si ρ_1 et ρ_2 sont différents, on n'obtient qu'un système minimum qui correspond au plus petit des nombres ρ_1 ou ρ_2.

On peut représenter les systèmes de solutions, sur un plan, au moyen d'un système d'axes rectangulaires; à toute solution correspond un point de coordonnées (x, y). On voit immédiatement que les points qui correspondent à toutes les solutions sont des points équidistants sur une droite AB déterminée par $OA = (c : a)$ et $OB = (c : b)$.

Les coordonnées du pied P de la perpendiculaire abaissée de l'origine O sur la droite AB sont positives et égales à

$$\frac{ac}{a^2 + b^2}, \quad \frac{bc}{a^2 + b^2}.$$

Le système minimum, en nombres entiers ou fractionnaires, correspond au pied P de cette perpendiculaire. On observera d'ailleurs que la méthode

x et y sont au moins égaux à 1. Pour les autres cas, considérons deux valeurs r et r' dont la somme soit égale à ab: nous allons démontrer que l'*on a*

$$\varpi(r) + \varpi(r') = 2 \quad \text{ou} \quad = 1,$$

suivant que r est, ou n'est pas, divisible par l'un des coefficients. Il suffit évidemment de supposer r non divisible par l'un des coefficients, attendu que de l'égalité

$$r + r' = ab$$

il résulte que r et r' sont en même temps divisibles ou non divisibles par a ou par b.

Soit $\varpi(r) = 1$; alors on a

$$0 < x' < b, \qquad 0 < y' < a,$$

et la seconde équation peut s'écrire

$$a(x + x') + b(y + y') = ab;$$

le nombre $(x + x')$ qui n'est pas nul, divisant b, est au moins égal à b; de même $(y + y')$ est au moins égal à a et le premier membre serait plus grand que le second. Au contraire, si $\varpi(r) = 0$, on a $y' < 0$, et l'on obtient pour la seconde équation le système positif

$$x = b - x', \qquad y = -y'.$$

Plus généralement, si l'on désigne par c et c' deux nombres non négatifs de somme nab, on a

$$\varpi(c) + \varpi(c') = n + 1 \quad \text{ou} \quad = n,$$

suivant que c est ou n'est pas divisible par l'un des coefficients.

Pour déterminer si $\varpi(r)$ est 0 ou 1, en supposant $0 \leqslant r < ab$, on peut employer un procédé direct, en formant tous les nombres de la forme $(ax + by)$, qui ne surpassent pas $\frac{1}{2}ab$. Si l'on suppose d'abord r divisible par l'un des coefficients, on voit que les entiers r divisibles par a, compris entre 0 et ab, sont en nombre $(b - 1)$; de même les entiers r divisibles par b sont en nombre $(a - 1)$; enfin 0 est le seul nombre divisible à la fois par a et par b; donc le nombre de ces valeurs de r pour lesquelles r est divisible par

l'un des coefficients est $(a+b-1)$. Les autres sont en nombre

$$ab-a-b+1 \quad \text{ou} \quad (a-1)(b-1);$$

par conséquent, il y a

$$\tfrac{1}{2}(a-1)(b-1)$$

valeurs de r pour lesquelles $\varpi(r)=0$. Ce théorème a été énoncé, mais démontré autrement, par CESARO (¹).

On a, par suite, la formule

$$\varpi(0)+\varpi(1)+\varpi(2)+\ldots+\varpi(ab-1)=ab-\tfrac{1}{2}(a-1)(b-1);$$

et, plus généralement,

$$\varpi(0)+\varpi(1)+\varpi(2)+\ldots+\varpi(qab-1)=\frac{q}{2}(qab+a+b-1).$$

Mais il restait à trouver la valeur de $\varpi(r)$, lorsque r est donné. Si l'on se reporte à la considération des systèmes minimums, et si l'on désigne par $+\rho_1$ le reste positif minimum et par $-\rho_2$ le reste négatif maximum de la division de

$$(-1)^{n-1}(a\alpha+b\beta)r \qquad \text{par} \qquad a^2+b^2,$$

on trouve, pour ces systèmes minimums,

$$\left\{\begin{aligned} x_1&=\frac{ar-b\rho_1}{a^2+b^2},\\ y_1&=\frac{br+a\rho_1}{a^2+b^2},\end{aligned}\right. \qquad \left\{\begin{aligned} x_2&=\frac{ar+b\rho_2}{a^2+b^2},\\ y_2&=\frac{br-a\rho_2}{a^2+b^2}.\end{aligned}\right.$$

Un seul de ces systèmes peut être positif; donc :

THÉORÈME. — *Pour que l'équation*

$$ax+by=r$$

soit possible en nombres entiers non négatifs, il faut et il suffit que l'un des nombres $(ar-b\rho_1)$, $(br-a\rho_2)$ *ne soit pas négatif, ou que leur produit ne soit pas positif.*

Les formules précédentes donnent d'ailleurs les deux systèmes minimums.

(¹) CESARO, *Sur diverses questions d'Arithmétique* (Soc. roy., Liège; 1883).

Exemple I. — Résoudre l'équation

$$35x + 24y = 201.$$

On a

$$a = 35, \quad b = 24, \quad r = 201;$$
$$\alpha = 16, \quad \beta = 11, \quad n = 3;$$

puis

$$t_1 = -92 \quad \text{et} \quad \rho_1 = 68;$$

d'où l'on tire le système positif

$$x = 3, \quad y = 4.$$

Exemple II. — Le nombre total des systèmes positifs des n équations

$$x + 2y = n - 1, \quad 2x + 3y = n - 2, \quad \ldots, \quad nx + (n+1)y = 0$$

est égal à n.

265. Sommes de fractions simples. — On appelle *fraction simple* toute fraction dont le dénominateur est une puissance quelconque d'un nombre premier a et dont le numérateur est compris entre o et a. Considérons d'abord une somme de fractions simples dont les dénominateurs sont des puissances différentes de a; soit, par exemple, la somme

$$\frac{x_1}{a^\alpha} + \frac{x_2}{a^{\alpha-1}} + \ldots + \frac{x_\alpha}{a},$$

dans laquelle $x_1, x_2, \ldots, x_\alpha$ sont des entiers positifs plus petits que a, en supposant que x_1 ne soit pas nul. On a

$$\frac{x}{a^\alpha} = \frac{x_1 + a x_2 + a^2 x_3 + \ldots + a^{\alpha-1} x_\alpha}{a^\alpha};$$

cette fraction est irréductible, puisque a ne divise pas x_1. Par conséquent, la somme de fractions simples, ayant pour dénominateurs des puissances différentes d'un même nombre premier a, est une fraction irréductible dont le dénominateur est égal au plus grand dénominateur de ces fractions.

Considérons une somme de fractions simples dont les dénominateurs sont des puissances différentes de deux nombres premiers a et b; en désignant par α et β les plus grands exposants de a et

de b dans les dénominateurs, cette somme sera, d'après ce qui précède,

$$\frac{x}{a^\alpha} + \frac{y}{b^\beta} = \frac{xb^\beta + ya^\alpha}{a^\alpha b^\beta};$$

la fraction qui représente cette somme est irréductible, puisque a premier à x et à b diviserait xb^β. Par suite, on a ce théorème général :

La somme de fractions simples dont les dénominateurs sont inégaux deux à deux est une fraction irréductible dont le dénominateur est égal au produit des plus hautes puissances des nombres premiers contenues dans les dénominateurs.

Réciproquement, *si deux sommes de fractions simples, dans chacune desquelles les dénominateurs sont inégaux deux à deux, sont égales, elles sont identiques.* En effet, les deux sommes sont des fractions irréductibles égales; par conséquent, les dénominateurs sont égaux et composés des mêmes facteurs premiers; de plus, dans chacune des deux sommes, les plus grands exposants des puissances d'un même nombre premier sont égaux.

Soit donc

$$\frac{x_1}{a^\alpha} + \frac{x_2}{a^{\alpha-1}} + \ldots + \frac{y_1}{b^\beta} + \ldots + \frac{z_1}{c^\gamma} + \ldots$$
$$= \frac{x'_1}{a^\alpha} + \frac{x'_2}{a^{\alpha-1}} + \ldots + \frac{y'_1}{b^\beta} + \ldots + \frac{z'_1}{c^\gamma} + \ldots;$$

si l'on multiplie les deux membres par $a^{\alpha-1} b^\beta c^\gamma \ldots$, on en déduit que $(x_1 - x'_1)$ est divisible par a; et puisque x et x' sont positifs et plus petits que a, on en conclut $x_1 = x'_1$. En supprimant les deux premières fractions égales, on démontre de même que $x_2 = x'_2$, ..., et ainsi de suite.

Si l'on étend le nom de *fractions simples* à des fractions dont les dénominateurs sont des puissances d'un entier $A > 1$, et dont les numérateurs sont plus petits que A, la proposition précédente subsiste, avec sa réciproque, pour des nombres quelconques A, B, C, ..., positifs et premiers entre eux deux à deux.

266. Décomposition des nombres fractionnaires en sommes de fractions simples. — Considérons d'abord le cas d'un nombre

fractionnaire irréductible dont le dénominateur est le produit de deux entiers positifs A et B premiers entre eux, et dont le numérateur N est un entier positif ou négatif, mais non nul. L'équation

$$AY + BX = N$$

possède une infinité de solutions; on a donc d'une infinité de manières la décomposition

$$\frac{N}{AB} = \frac{X}{A} + \frac{Y}{B}.$$

Soient x et y les restes positifs des divisions de X par A et de Y par B; nous obtenons

$$\frac{N}{AB} = \frac{x}{A} + \frac{y}{B} + E,$$

E désignant un nombre entier positif, nul ou négatif; mais x est compris entre zéro et A, et y entre zéro et B.

Remplaçons B par le produit BC de deux nombres positifs premiers à A et premiers entre eux, nous aurons

$$\frac{N}{ABC} = \frac{x}{A} + \frac{y}{BC} + E;$$

en décomposant la fraction $(y : BC)$, on déduit

$$\frac{N}{ABC} = \frac{x}{A} + \frac{y'}{B} + \frac{z'}{C} + E',$$

et ainsi de suite. Par conséquent, toute fraction irréductible dont le dénominateur est le produit d'entiers positifs et premiers entre eux deux à deux peut être décomposée en une somme de fractions, comprises entre o et 1, augmentée d'un entier positif, nul ou négatif.

Il résulte d'ailleurs du numéro précédent que cette décomposition est unique, bien qu'elle puisse s'effectuer de plusieurs manières différentes.

Remplaçons A par A^α, B par B^β, ...; nous aurons donc l'égalité

$$(1) \qquad \frac{N}{A^\alpha B^\beta C^\gamma \ldots} = \frac{x}{A^\alpha} + \frac{y}{B^\beta} + \frac{z}{C^\gamma} + \ldots + E,$$

dans laquelle toutes les fractions du second membre sont irréduc-

tibles et comprises entre o et 1. Divisons x par A, puis le quotient par A, et ainsi de suite, comme s'il s'agissait d'écrire le nombre x dans le système de numération de base A, et supposons (n° 30)

$$x = x_1 + Ax_2 + A^2x_3 + \ldots + A^{\alpha-1}x_\alpha,$$

nous obtiendrons, en divisant les deux membres par A^α,

$$\frac{x}{A^\alpha} = \frac{x_1}{A^\alpha} + \frac{x_2}{A^{\alpha-1}} + \frac{x_3}{A^{\alpha-2}} + \ldots + \frac{x_\alpha}{A};$$

les numérateurs $x_1, x_2, x_3, \ldots, x_\alpha$ sont des entiers positifs, plus petits que A, qui peuvent être nuls, à l'exception du premier x_1. En opérant de même pour les autres fractions du second membre de l'égalité (1), on en déduit

$$\begin{aligned}\frac{N}{A^\alpha B^\beta C^\gamma \ldots} = E &+ \frac{x_1}{A^\alpha} + \frac{x_2}{A^{\alpha-1}} + \ldots + \frac{x_\alpha}{A} \\ &+ \frac{y_1}{B^\beta} + \frac{y_2}{B^{\beta-1}} + \ldots + \frac{y_\beta}{B} \\ &+ \frac{z_1}{C^\gamma} + \frac{z_2}{C^{\gamma-1}} + \ldots + \frac{z_\gamma}{C} \\ &+ \ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

Donc, tout nombre fractionnaire irréductible dont le dénominateur est le produit de puissances d'entiers positifs A, B, C, ..., premiers entre eux deux à deux, est décomposable en une somme d'un entier et de fractions ayant pour dénominateurs les puissances de A, B, C, ..., et pour numérateurs des entiers positifs respectivement plus petits que A, B, C, ... Si ces nombres ne peuvent être décomposés en produits d'autres nombres, la décomposition est unique, d'après le numéro précédent; mais elle peut être obtenue de diverses manières.

En particulier, si l'on remplace A, B, C, ... par des nombres premiers $a, b, c, \ldots$, inégaux deux à deux, on a ce théorème :

Toute fraction irréductible est, d'une seule manière, égale à la somme de fractions simples, augmentée d'un entier positif, nul, ou négatif.

Exemple I. — Décomposer en fractions simples la fraction $\frac{1}{3.5.17}$.
On trouve $\frac{1}{3} + \frac{1}{5} + \frac{8}{17} - 1$.

Lorsque l'on sait diviser géométriquement la circonférence en $p, q, r, \ldots$ parties égales, on saura la diviser en $pqr\ldots$ parties égales, si les nombres $p, q, r, \ldots$ sont impairs et premiers entre eux deux à deux, et, par suite, on saura la diviser en $2^{\alpha}pqr\ldots$ parties égales. Les seuls nombres $p, q, r, \ldots$ connus actuellement sont les nombres premiers

$$3,\ 5,\ 17,\ 257,\ 65537,$$

et le nombre suivant serait [illegible], qui a [illegible] chiffres, si l'on pouvait démontrer que ce nombre est premier (voir n° 36, *Ex. I*).

Exemple II. — Décomposer en fractions simples le nombre [illegible].

On trouve (*Diag. Arith.*, n° 317)

[illegible]

NOTES ET ADDITIONS.

I. — Sur la partition des polygones (n° 57).

D'après une communication qui nous a été adressée par M. Cayley, le théorème énoncé à la page 93 doit être attribué à Kirkmann, qui l'a démontré dans son Mémoire : *On the k-partitions of the r-gone*, publié dans les *Philosophical Transactions* (t. CXLVII; Londres, 1857).

D'autre part, nous avons reçu de M. Élie Perrin, professeur à l'École J.-B. Say, les remarques suivantes : Soit ABC...HKL un polygone de $(n+1)$ côtés; choisissons AB pour base principale, et désignons par a_1, a_2, a_3, ..., a_n les côtés BC, CD, DE, ..., KA. Si, par exemple, le triangle ABG fait partie d'une décomposition, le sommet G décompose le périmètre BCD...GHK en deux polygones ayant pour bases principales BG et AG, qui remplacent AB; de même, si le triangle BGE fait partie d'une décomposition, il sépare le polygone BCDEG en deux autres, et ainsi de suite; on classe ainsi, *dichotomiquement*, les $(n-1)$ sommets du polygone, autres que A et B.

Plaçons, sur une ligne horizontale, les côtés

$$a_1,\quad a_2,\quad a_3,\quad \ldots,\quad a_n,$$

et supposons, pour fixer les idées, que n est égal à 8. Si le point G fait partie de la décomposition, il sépare a_5 de a_6 et nous représenterons cette première décomposition par

$$(a_1, a_2, a_3, a_4, a_5),\ (a_6, a_7, a_8);$$

puis, si BGE fait partie de la décomposition, nous séparerons a_1, ..., a_5 en deux par

$$((a_1, a_2, a_3), (a_4, a_5)),\ (a_6, a_7, a_8),$$

et ainsi de suite. Par conséquent, si l'on considère la décomposition du polygone de 9 côtés, dans laquelle on a tracé les diagonales GK, GA, GB, GE, BE, CE, on peut représenter cette décomposition par le symbole

$$(((a_1), (a_2, a_3)), (a_4, a_5)),\ ((a_6, a_7), (a_8)),$$

ou

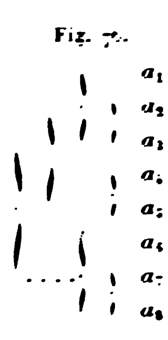
$$\overline{\overline{\overline{a_1,\ \overline{a_2,\ a_3}},\ \overline{a_4,\ a_5}},\ \overline{\overline{a_6,\ a_7},\ a_8}}.$$

En général, à toute décomposition d'un polygone de $n-1$ côtés en $n-1$ triangles, correspond une manière d'obtenir le produit de n facteurs $a_1, a_2, a_3, \ldots, a_n$, par $n-1$ multiplications de deux facteurs, en effectuant suivant l'ordre des indices, et inversement. Par conséquent :

Le nombre des manières d'effectuer le produit de n facteurs $a_1, a_2, \ldots, a_n$, au moyen de $n-1$ multiplications de deux facteurs, pris dans l'ordre des indices, est égal au nombre des décompositions d'un polygone convexe de $n-1$ côtés en triangles, par des diagonales qui ne se coupent pas à l'intérieur du polygone.

On en déduit facilement cet autre théorème : *Le nombre des manières d'effectuer le produit de n facteurs, au moyen de $n-1$ multiplications de deux facteurs pris dans un ordre quelconque, est égal au produit du nombre des décompositions du polygone de $n-1$ côtés en triangles, par le nombre $n!$ des permutations des n facteurs.*

Fig. 7.



La figure ci-jointe nous montre encore que le nombre des manières d'interpréter une fraction étagée de n termes (n° 82, *Ex. II*) est égal au nombre des décompositions d'un polygone de $(n-1)$ côtés en triangles.

Et ainsi le nombre des classements, par voie dichotomique, de n objets rangés dans un certain ordre, est égal au nombre des décompositions d'un polygone de $(n-1)$ côtés en triangles, par $(n-1)$ diagonales qui ne se coupent pas à l'intérieur du polygone.

II. Sur le problème des rencontres (n° 123).

Le nombre Q_n des permutations de n lettres, où aucune lettre n'occupe la place que lui assigne son rang dans l'alphabet, est égal au nombre des substitutions irréductibles de n lettres.

Cette même question a été traitée par LAPLACE et généralisée, au moyen de la théorie des fonctions génératrices, dans la *Théorie analytique des Probabilités* (*Œuvres*, t. VII, p. 242).

De la formule

$$Q_{n+1} = (n+1)Q_n - (-1)^{n+1},$$

on déduit, en remplaçant n successivement par 1, 2, ..., n, et en faisant la somme des égalités obtenues,

$$Q_{n+1} = \Sigma n Q_n + \text{const.},$$

la constante étant égale à 0 ou à 1, suivant que n est pair ou impair.

On peut obtenir diverses propriétés arithmétiques des nombres Q_n. On remarque d'abord que deux nombres consécutifs sont premiers entre eux, par suite de la formule (2) du n° 123. De plus, Q_{n+1} est divisible par n, comme cela résulte de la première formule de la page 213. De la formule symbolique

$$(P + x)^n \triangleq (Q + x + 1)^n,$$

on déduit la formule générale

$$f(P + x) \triangleq f(Q + x + 1),$$

et, par exemple, en supposant

$$f(z) = z^r (z - 1)^s,$$

il vient

$$(P + x)^r (P + x - 1)^s \triangleq (Q + x + 1)^r (Q + x)^s,$$

et pour $x = 0$

$$P^r (P - 1)^s \triangleq Q^s (Q + 1)^r.$$

Si l'on remplace r par un nombre premier p, en observant que P_n est divisible par p, pour $n \geqq p$, et en tenant compte des restes du triangle arithmétique, il vient

$$Q_{p+s} \equiv - Q_s \qquad (\text{mod. } p);$$

on en tire, plus généralement,

$$Q_{hp+s} \equiv (-1)^h Q_s \qquad (\text{mod. } p),$$

et ainsi les restes de Q_n par p se reproduisent périodiquement.

III. — Sur le problème des ménages (n° 123).

Nous désignerons par F et H, avec les indices de 1 à n, les n femmes et leurs maris respectifs; puis, par

λ_n le nombre des permutations des n ménages qui sont conformes à l'énoncé;

μ_n » qui présentent le seul défaut de finir par 1;

ν_n le nombre des permutations qui présentent un seul défaut, à l'exception de commencer ou de finir par 1, ou de finir par n;
ρ_n » qui se terminent par 1 et présentent un seul autre défaut.

Supposons que les n ménages soient assis autour de la table dans l'une des λ_n dispositions cherchées et que survienne un ménage que nous désignerons par F_{n+1} et H_{n+1}; alors les convives se serrent de manière à ouvrir deux nouvelles places formant un intervalle que nous pouvons imaginer situé immédiatement à gauche de F_1. Alors F_{n+1} se place dans cet intervalle, et si son mari s'y plaçait, la permutation serait fautive; mais le mari H_{n+1} peut changer de place avec les n maris, à l'exception de deux, H_1 et celui qui est à la gauche de F_1. Par conséquent, par cette intercalation, nous obtenons $(n-2)\lambda_n$ dispositions. Mais on peut encore obtenir d'autres permutations, conformes à l'énoncé, en commençant par les permutations fautives de n ménages, que nous avons désignées par μ_n, ν_n, ρ_n.

1° Supposons que, dans la permutation qui précède l'arrivée des nouveaux venus, le mari H_1 soit à la gauche de sa femme F_1; dans ce cas, le ménage d'indice $(n+1)$ peut se placer à la gauche de F_1: mais le mari H_{n+1} doit échanger sa place avec l'un quelconque des maris, à l'exception de H_1; on obtient ainsi $(n-1)\mu_n$ permutations des ménages.

2° Supposons que la permutation qui précède l'arrivée des nouveaux venus soit une de celles que nous avons désignées par ν_n, alors le ménage d'indice $(n+1)$, se plaçant à la gauche de F_1, la permutation est fautive; mais on ne peut la rendre conforme à l'énoncé que par l'échange de H_{n+1} avec le mari qui se trouvait à côté de sa femme; on a ainsi ν_n permutations des $(n+1)$ ménages, distinctes des précédentes.

3° Si la permutation qui précède l'arrivée du $(n+1)^{\text{ième}}$ ménage est une de celles que nous avons désignées par ρ_n, le premier défaut se trouve corrigé par l'intercalation de F_{n+1} à la gauche de F_1, et le second défaut par H_{n+1}, qui remplace le mari qui se trouvait à côté de sa femme, tandis que celui-ci vient se placer entre F_1 et F_{n+1}; par suite, ρ_n permutations distinctes des précédentes.

Inversement, si l'on considère une permutation quelconque λ_{n+1} de $(n+1)$ ménages, conforme aux conditions de l'énoncé, le départ du ménage $(n+1)$ conduit à l'une des quatre dispositions que nous avons désignées par λ_n, μ_n, ν_n et ρ_n. On a donc la formule

$$(1) \qquad \lambda_{n+1} = (n-2)\lambda_n + (n-1)\mu_n + \nu_n + \rho_n.$$

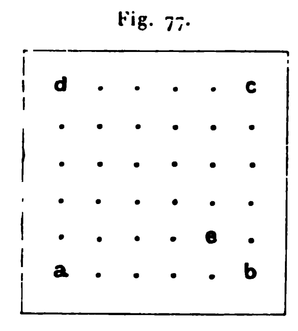
Pour obtenir d'autres formules, nous reprendrons la figuration sur un échiquier de n^2 cases (p. 215), en désignant par a, b, c, d, e, les cases que nous aurons à considérer plus spécialement (*fig.* 77). Les permuta-

tions sans défaut (λ_n) sont celles qui correspondent au problème des n tours placées sur les cases de l'échiquier, à l'exception des cases de la diagonale ac, des cases situées immédiatement au-dessus, et de la case b. Nous supposerons toutes les cases *blanches*, à l'exception de celles que nous venons d'indiquer et que nous considérerons comme *noires*.

Les dispositions dans lesquelles une tour occupe la case a, et les $(n-1)$ autres tours sont sur des cases blanches, ont été désignées par μ_n; celles dans lesquelles une seule tour occupe une case noire autre que a, b, c, sont des ν_n; enfin, celles où une tour occupe une case noire autre que a, b, c et où, en outre, une tour occupe la case a, constituent la catégorie ρ_n.

Si nous considérons l'une des permutations μ_n et si nous supprimons par la pensée la ligne et la colonne renfermant la case a, il reste un échiquier de $(n-1)^2$ cases sur lequel les $(n-1)$ autres tours forment une

Fig. 77.



Problème des ménages.

certaine permutation. Si la case e n'est pas occupée, cette permutation rentre dans la catégorie λ_{n-1}, et si la case e est occupée, elle rentre dans la catégorie μ_{n-1}. On a donc

$$(2) \qquad \mu_n = \lambda_{n-1} + \mu_{n-1}.$$

Si nous considérons l'une des permutations ν_n, elle présente cette circonstance que l'une des cases noires, autre que a, b ou c, est occupée par une tour. Or, par des permutations circulaires des colonnes, puis des lignes de l'échiquier, on peut amener cette tour à occuper la position a et former ainsi l'une des permutations μ_n; mais il y a sur l'échiquier $(2n-3)$ cases noires autres que a, b, c; on a donc

$$(3) \qquad \nu_n = (2n-3)\mu_n.$$

Enfin, dans une permutation ρ_n, la case a est toujours occupée. Si la case d est occupée, la permutation figurée qui reste lorsque l'on supprime

la ligne et la colonne contenant a, appartient à la catégorie ρ_{n-1}, comme on le reconnaît facilement en tournant l'échiquier d'un demi-tour autour de son centre. Si la case d n'est pas occupée, on peut toujours amener la case fautive à occuper cette place extrême par des permutations convenables des lignes et des colonnes, ce qui donne une permutation μ_{n-1}; mais comme il y a $(2n-3)$ cases noires que l'on peut amener en d, on en conclut la formule

$$(4)\qquad \rho_n = (2n-3)\mu_{n-1} + \rho_{n-1}.$$

Des formules (1) et (3), on déduit

$$(5)\qquad \lambda_{n+1} = (n-2)\lambda_n + (3n-4)\mu_n + \rho_n.$$

Au moyen des diverses relations qui précèdent, et des valeurs initiales

$$\begin{cases}\lambda_3 = 1,\\ \lambda_4 = 2,\end{cases}\quad \begin{cases}\mu_3 = 0,\\ \mu_4 = 1,\end{cases}\quad \begin{cases}\nu_3 = 0,\\ \nu_4 = 1,\end{cases}\quad \begin{cases}\rho_3 = 1,\\ \rho_4 = 1,\end{cases}$$

on peut former le Tableau des valeurs de λ_n, μ_n, ν_n, ρ_n pour les premières valeurs de n; les différences des λ et des ρ vérifient les formules (2) et (4), que l'on peut écrire

$$\lambda_{n-1} = \Delta\mu_{n-1}, \qquad \mu_{n-1} = \frac{\Delta\rho_{n-1}}{2n-3}.$$

En donnant à n des valeurs successives, on déduit les formules

$$(6)\qquad (n-1)\lambda_{n+1} = (n^2-n+1)(\lambda_n + \lambda_{n-1}) + n\lambda_{n-2},$$

$$(7)\qquad \lambda_{n+1} = (n+1)\lambda_n + 2\lambda_{n-1} - (n-3)\lambda_{n-2} - \lambda_{n-3},$$

où n'entrent plus que des λ. Enfin, il y a lieu de noter la formule

$$(8)\qquad \mu_{n+2} = n(\mu_{n+1} + \mu_n) + \mu_{n-1}.$$

Les formules et les démonstrations précédentes ont été obtenues, pour la première fois, par M. Laisant. D'un autre côté, M. C. Moreau, colonel d'artillerie, qui est parvenu aux mêmes résultats, a encore indiqué les formules suivantes. On peut écrire la relation (6) sous la forme

$$\begin{aligned}(n-1)\lambda_{n+1} - (n+1)(n-1)\lambda_n - (n+1)\lambda_{n-1}\\ = -[(n-2)\lambda_n - n(n-2)\lambda_{n-1} - n\lambda_{n-2}];\end{aligned}$$

on peut donc poser

$$(n-2)\lambda_n - n(n-2)\lambda_{n-1} - n\lambda_{n-2} = K(-1)^{n-1},$$

en désignant par K une constante que l'on trouve égale à 4. Ainsi

$$(9)\qquad (n-1)\lambda_{n+1} = (n^2-1)\lambda_n + (n+1)\lambda_{n-1} + 4(-1)^n.$$

L'observation du Tableau qui contient les premières valeurs de λ conduit à poser

$$(10)\qquad \lambda_n - 2(-1)^n = n\theta_n,$$

et l'équation précédente donne

$$(11)\qquad \theta_{n+1} = n\theta_n + \theta_{n-1} + 2(-1)^n.$$

La formule (11) permet de calculer rapidement les valeurs de θ_n; on a ensuite celles de λ_n par la formule

$$\lambda_n = \theta_{n+1} - \theta_{n-1};$$

on trouve ainsi, pour les premières valeurs de n,

n.	θ_n.	λ_n.
4	0	2
5	3	13
6	13	80
7	83	579
8	592	4738
9	4821	43387
10	43979	4 39792
11	4 44613	48 90741
12	49 34720	592 16642
13	596 61255	7755 96313
14	7805 31033	1 09274 34464
15	1 09870 95719	16 48064 35783
16	16 55869 66816	264 93914 69058
17	266 03785 64777	4522 64356 01207
18	4539 20225 68023	81705 64062 24416
19	81971 67847 89193	15 57461 89109 94665
20	15 62001 09335 62688	312 40021 86712 53762
21	313 21993 54560 42955	....

IV. — Sur les nombres d'HAMILTON (n° 81).

Considérons le Tableau suivant; il est formé d'étages successifs, séparés par une barre horizontale; dans chaque étage, un nombre quelconque est égal au nombre placé immédiatement au-dessus, augmenté de tous ceux qui précèdent celui-ci dans la même ligne. Cette loi subsiste quand on passe d'un étage à l'étage inférieur, excepté pour les premières colonnes

de chaque étage, qui sont formées par la suite naturelle des nombres en-

1	0	0	0	0	0	0	...
	1	1	1	1	1	1	...
		2	3	4	5	6	..
		1	5	9	14	20	...
			6	15	29	49	...
			5	21	50	99	...
			4	26	76	175	...
			3	30	106	281	...
			2	33	139	420	...
			1	35	174	594	...
				36	210	804	...
				35	246	1050	..
				34	281	1331	...
				.	.	.	...
				.	.	.	...

Les nombres d'Hamilton.

tiers positifs et décroissants jusqu'à 1. Les premiers nombres de chaque étage, que nous désignerons par a_0, a_1, a_2, a_3, ..., forment la suite

$$1,\ 1,\ 2,\ 6,\ 36,\ 876,\ \dots;$$

si l'on pose

$$s_{n+1} = a_0 + a_1 + a_2 + \dots + a_n \quad \text{et} \quad H_n = s_n + 1,$$

on obtient, pour H_1, H_2, H_3, ..., les nombres renfermés dans le Tableau suivant :

H_n.	n.
2	1
3	2
5	3
11	4
47	5
923	6
4 09619	7
8 37632 06255	8
35 08125 90629 08587 98171	9
615 34736 87096 57875 84485 22809 27507 75204 33167	10

Les nombres H, que M. SYLVESTER a appelés *nombres d'Hamilton*, jouent un très grand rôle dans la théorie des équations ([1]).

Le calcul des nombres du Tableau précédent a été effectué au moyen d'une formule très remarquable, due à M. J. HAMMOND.

Soit

$$\begin{aligned} 1 + x + x^2 + x^3 + x^4 + \ldots &= g_0(x), \\ 2x + 3x^2 + 4x^3 + 5x^4 + \ldots &= g_1(x), \\ 6x^2 + 15x^3 + 29x^4 + \ldots &= g_2(x), \\ 36x^3 + 210x^4 + \ldots &= g_3(x), \end{aligned}$$

et ainsi de suite; en général,

$$a_n x^n + b_n x^{n+1} + c_n x^{n+2} + d_n x^{n+3} + \ldots = g_n(x).$$

On multiplie $g_n(x)$ par le développement de la puissance de $(1-x)$ d'exposant égal à $-a_n$; si l'on compare le résultat au développement de $g_{n+1}(x)$, en tenant compte de la loi de formation,

$$\begin{aligned} a_{n+1} &= b_n + \frac{a_n(a_n+1)}{1.2}, \\ b_{n+1} &= c_n + a_n b_n + \frac{a_n(a_n+1)(2a_n+1)}{1.2.3}, \\ c_{n+1} &= d_n + a_n c_n + \frac{a_n(a_n+1)(a_n+2)(3a_n+1)}{1.2.3.4}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

on a

$$g_{n+1}(x) = \frac{g_n(x)}{(1-x)^{a_n}} - \frac{x^{n-1}}{(1-x)^{a_n-1}} + x^{n-1}(1-x).$$

Multiplions les deux membres par $(1-x)^{s_{n+1}}$, il vient

$$\begin{aligned} &(1-x)^{s_{n+1}} g_{n+1}(x) - (1-x)^{s_n} g_n(x) \\ &\quad = x^{n-1}(1-x)^{s_{n+1}+1} - x^{n-1}(1-x)^{s_n+1}. \end{aligned}$$

Remplaçons successivement n par $0, 1, 2, \ldots, (n-1)$, et ajoutons les identités obtenues; il vient, après quelques transformations,

$$\begin{aligned} &(1-x)^{s_n} g_n(x) - (1-x)^{-1} + x^{-1}(1-x) - x^{n-1}(1-x)^{s_n+1} \\ &\quad = x^{n-2}(1-x)^{s_n+2} + x^{n-3}(1-x)^{s_{n-1}+2} + \ldots \\ &\quad\quad + x^{n-4}(1-x)^{s_{n-2}+2} + \ldots + x^{-1}(1-x)^{s_1+2}. \end{aligned}$$

([1]) SYLVESTER, *Sur les nombres dits de Hamilton*. Congrès de Toulouse, 1887, p. 165. — SYLVESTER et HAMMOND, *On Hamilton's Numbers*, dans les *Philosophical Transactions*, vol. CLXXVIII, p. 285-312, et vol. CLXXIX, p. 65-71. Londres, 1887.

En égalant les coefficients de x^n dans les deux membres, on obtient ainsi la formule de M. HAMMOND

$$H_{n+1} - 1 = \frac{H_n(H_n - 1)}{2!} - \frac{H_{n-1}(H_{n-1} - 1)(H_{n-1} - 2)}{3!} + \ldots$$
$$+ (-1)^{n+1} \frac{H_1(H_1 - 1)(H_1 - 2)\ldots(H_1 - n)}{(n+1)!}.$$

En multipliant les deux membres de l'identité précédente par $(1 - x)$ et en identifiant les coefficients de x^n, on trouve, après avoir posé $l_n = H_n + 1$, la formule donnée par M. SYLVESTER

$$1 - l_{n-1} + \frac{l_{n-2}(l_{n-2} - 1)}{2!} - \ldots + (-1)^n \frac{l_0(l_0 - 1)\ldots(l_0 - n + 1)}{n!} = 0$$

ou, en se servant de la notation des combinaisons,

$$1 - C^1_{l_{n-1}} + C^2_{l_{n-2}} - C^3_{l_{n-3}} + \ldots = 0.$$

V. — Sur les réseaux d'un quinconce (n° 190, *Ex. II*).

Quelles que soient les dimensions du quinconce, on peut en séparer tous les sommets par deux séries de lignes parallèles (*fig.* 78), et de telle sorte que chaque sommet occupe le centre d'un carré formé par le réseau des deux systèmes de parallèles. Puisque tous les sommets du réseau sont des points d'ordre pair (2 ou 4), ce réseau peut toujours être décrit d'un seul trait (n° 59); mais, conformément à l'énoncé, les lignes des deux systèmes de parallèles doivent être décrites d'un seul trait continu. Soient p et q les nombres des points contenus sur les côtés AT et AG du rectangle; de plus, supposons p et q premiers entre eux; sur la figure on a $p = 5$ et $q = 7$.

Supposons que la figure soit repliée autour de la ligne HL, puis que l'on replie de nouveau la figure autour du côté inférieur, et ainsi de suite: on forme donc de deux en deux le même dessin et de deux en deux des images du dessin. Cela posé, en partant de A, on décrit le chemin AB en descendant de p lignes, puis le chemin BCD, dont on remplace la partie CD par sa symétrique, de manière à descendre toujours entre les deux côtés AG et TM du rectangle. En partant du côté gauche, pour y revenir après réflexion sur le côté droit, on descend donc de $2q$ lignes sur l'échiquier indéfini. Pour obtenir les numéros des points de brisure sur AG ou son prolongement, on forme donc la progression arithmétique, de raison $2p$,

$$0, \quad 2p, \quad 4p, \quad 6p, \quad \ldots.$$

Mais si l'on veut obtenir les numéros correspondants sur le rectangle primitif de la figure, on prend les restes de ces nombres par $2q$; alors

deux cas peuvent se présenter, suivant que le reste r, toujours pair, ne dépasse pas $(q-1)$ ou est plus grand que $(q-1)$; dans le premier cas, on conserve le reste obtenu, car le numéro de brisure correspond à un

Fig. 78.

rectangle de même orientation que le rectangle primitif; dans le second cas, si l'on a

$$r > q - 1,$$

le point de brisure se trouve dans un rectangle symétrique du premier; alors on remplace r par son complément à $(2q-1)$.

Ainsi, dans l'exemple, on forme les nombres

$$0,\ 10,\ 20,\ 30,\ 40,\ 50,\ 60,\ 70;$$

les restes par 14 sont

$$0,\ 10,\ 6,\ 2,\ 12,\ 8,\ 4,\ 0.$$

On conserve les restes 0, 6, 2, 4, et l'on remplace les autres par leurs compléments à 13; on a ainsi

$$0,\ 3,\ 6,\ 2,\ 1,\ 5,\ 4,\ 0.$$

Donc on passe successivement par les sommets

$$\mathrm{A},\quad \mathrm{D},\quad \mathrm{G},\quad \mathrm{K},\quad \mathrm{N},\quad \mathrm{S},\quad \mathrm{V},\quad \mathrm{A},$$

et l'on revient au point de départ après avoir passé par tous les sommets du côté AG. Il en est toujours ainsi lorsque p et q sont premiers entre eux, car les restes de

$$0,\quad 2p,\quad 4p,\quad 6p,\quad \ldots,\quad 2qp$$

par $2q$ sont tous pairs et différents; en complétant à $(2q-1)$ ceux qui surpassent $(q-1)$, on obtient des nombres impairs tous différents. On forme donc la suite des nombres de 0 à $(q-1)$. D'ailleurs le même raisonnement s'applique sur les autres côtés du rectangle.

Lorsque les nombres p et q ont un plus grand codiviseur d, le réseau se trouve formé de d contours continus de même longueur. En effet, posons

$$p = p'd \qquad \text{et} \qquad q = q'd,$$

p' et q' étant premiers entre eux. Alors le terme de rang q' dans la progression arithmétique

$$0,\quad 2p,\quad 4p,\quad \ldots,\quad 2q'p$$

donne 0 pour reste, et le contour commençant en A ne rencontre plus que q' points du côté AG; en supprimant ce contour, on prend un autre des sommets sur AG et l'on forme de même un second contour au moyen d'une progression arithmétique de raison $2p$, et ainsi de suite. C. Q. F. D.

Cette démonstration est due à M. Élie Perrin.

VI. — Sur la sommation des indicateurs (nº 224).

Si l'on désigne par $\Sigma\varphi(n)$ la somme des indicateurs des n premiers nombres et par $p, q, r, \ldots$ tous les nombres premiers qui ne surpassent pas n, on a la formule

$$(1)\quad \begin{cases} 2\sum \varphi(n) = n^2+1-\sum\left(\mathrm{E}\,\dfrac{n}{p}\right)^2+\sum\left(\mathrm{E}\,\dfrac{n}{pq}\right)^2 \\ \qquad\qquad -\sum\left(\mathrm{E}\,\dfrac{n}{pqr}\right)^2+\ldots. \end{cases}$$

On a, par exemple, pour $n=6$,

$$p=2,\qquad q=3,\qquad r=5,$$

$$\mathrm{E}\,\frac{6}{2}=3,\qquad \mathrm{E}\,\frac{6}{3}=2,\qquad \mathrm{E}\,\frac{6}{5}=1,$$

$$\mathrm{E}\,\frac{6}{2.3}=1,\qquad \mathrm{E}\,\frac{6}{2.5}=0,\qquad \mathrm{E}\,\frac{6}{3.5}=0,\qquad \mathrm{E}\,\frac{6}{2.3.5}=0;$$

par suite,

$$2\Sigma\varphi(6) = 36 + 1 - 9 - 4 - 1 + 1 + 0 + 0 - 0 = 24,$$

et l'on a

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) = 12.$$

Pour démontrer la formule (1), il suffit donc de faire voir que, si elle est vérifiée pour les $(n-1)$ premiers entiers, elle subsiste pour les n premiers. Lorsque l'on passe de $(n-1)$ à n, le second membre de cette formule augmente de

$$(2)\quad \left\{\begin{aligned} &n^2 - (n-1)^2 - \sum\left[\left(\mathrm{E}\,\frac{n}{p}\right)^2 - \left(\mathrm{E}\,\frac{n-1}{p}\right)^2\right] \\ &\qquad + \sum\left[\left(\mathrm{E}\,\frac{n}{pq}\right)^2 - \left(\mathrm{E}\,\frac{n-1}{pq}\right)^2\right] - \ldots; \end{aligned}\right.$$

mais si l'on observe que la différence

$$\mathrm{E}\,\frac{n}{x} - \mathrm{E}\,\frac{n-1}{x}$$

est égale à 1 ou à 0, suivant que x est ou n'est pas diviseur de n, et si l'on désigne par a, b, c, ... les diviseurs premiers de n et par μ leur nombre, l'expression (2) devient

$$(3)\quad \left\{\begin{aligned} &2n - 1 - \sum \mathrm{E}\left(\frac{2n}{a} - 1\right) + \sum \mathrm{E}\left(\frac{2n}{ab} - 1\right) \\ &\qquad - \sum \mathrm{E}\left(\frac{2n}{abc} - 1\right) + \ldots \end{aligned}\right.$$

ou encore

$$2n\left(1 - \sum\frac{1}{a} + \sum\frac{1}{ab} - \sum\frac{1}{abc} + \ldots\right) - \left(1 - C_\mu^1 + C_\mu^2 - C_\mu^3 + \ldots\right),$$

c'est-à-dire $2\varphi(n)$, puisque la somme alternée des coefficients du binôme est égale à zéro.

La formule (1) a été donnée par M. Perott, dans le *Bulletin des Sciences mathématiques* (t. IV); la démonstration précédente nous a été communiquée par M. J. Hammond.

VII. — Sur les permutations circulaires avec répétition (n° 224).

Lorsque n désigne un entier quelconque, le nombre des permutations rectilignes de n objets tous différents est égal à $n!$ et le nombre des permutations circulaires est égal à $(n-1)!$

Mais il n'en est plus ainsi lorsque les objets ne sont pas tous distincts; si l'on suppose $\alpha, \beta, \gamma, \ldots, \lambda$ objets respectivement égaux à $a, b, c, \ldots l$ et si l'on fait

$$n = \alpha + \beta + \gamma + \ldots + \lambda,$$

le nombre des permutations rectilignes est

$$R(n) = \frac{n!}{\alpha!\,\beta!\,\gamma!\ldots\lambda!}; \tag{1}$$

mais il reste à déterminer le nombre $G(n)$ des permutations circulaires. Si les n objets sont tous différents, on a la formule

$$nG(n) = R(n), \tag{2}$$

parce que chaque permutation circulaire peut être ouverte à n places pour former des permutations rectilignes distinctes. La formule (2) subsiste encore si les nombres $\alpha, \beta, \gamma, \ldots, \lambda$ sont premiers entre eux; mais, si ces nombres ont un codiviseur autre que l'unité, il y aura des permutations circulaires qui se composeront de groupes identiques et qui produiront, par leur ouverture, moins de n permutations rectilignes correspondantes. Ainsi, par exemple, soient les quatre objets a, a, b, b, la permutation circulaire

$$\begin{array}{ccc} & a & \\ b & & a \\ & b & \end{array} \quad \text{donne les quatre permutations rectilignes} \quad \left\{ \begin{array}{l} aabb, \\ abba, \\ bbaa, \\ baab, \end{array} \right.$$

et la permutation circulaire

$$\begin{array}{ccc} & a & \\ b & & b \\ & a & \end{array} \quad \text{ne donne que deux permutations rectilignes} \quad \left\{ \begin{array}{l} abab, \\ baba. \end{array} \right.$$

Désignons par D le plus grand codiviseur des nombres $\alpha, \beta, \gamma, \ldots, \lambda$ et par $p, q, r, \ldots$ les facteurs premiers qu'il contient. Si l'on retranche de $G(n)$ et de $R(n)$ toutes les permutations qui peuvent se décomposer en groupes égaux, les permutations rectilignes qui restent sont n fois plus nombreuses que les permutations circulaires correspondantes; par conséquent, les deux expressions

$$G(n) - \sum G\left(\frac{n}{p}\right) + \sum G\left(\frac{n}{pq}\right) - \ldots \pm G\left(\frac{n}{pqr\ldots}\right),$$

$$\frac{1}{n}\left[R(n) - \sum R\left(\frac{n}{p}\right) + \sum R\left(\frac{n}{pq}\right) - \ldots \pm R\left(\frac{n}{pqr\ldots}\right)\right]$$

sont égales. Posons, pour abréger, $Q(x) = \frac{1}{x} R(x)$, on a donc la formule

$$(3)\quad \left\{ \begin{aligned} & G(n) - \sum G\left(\frac{n}{p}\right) + \sum G\left(\frac{n}{pq}\right) - \ldots \\ & = Q(n) - \sum \frac{1}{p} Q\left(\frac{n}{p}\right) + \sum \frac{1}{pq} Q\left(\frac{n}{pq}\right) - \ldots . \end{aligned} \right.$$

Si nous supposons d'abord D égal à un nombre premier p, au produit de deux nombres premiers p et q, ou à une puissance p^{ϖ} d'un nombre premier, nous trouvons respectivement

$$(4)\quad G(n) = Q(n) + \left(1 - \frac{1}{p}\right) Q\left(\frac{n}{p}\right),$$

$$(5)\quad \left\{ \begin{aligned} G(n) = Q(n) & + \left(1 - \frac{1}{p}\right) Q\left(\frac{n}{p}\right) + \left(1 - \frac{1}{q}\right) Q\left(\frac{n}{q}\right) \\ & + \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) Q\left(\frac{n}{pq}\right), \end{aligned} \right.$$

$$(6)\quad \left\{ \begin{aligned} G(n) = Q(n) & + \left(1 - \frac{1}{p}\right) Q\left(\frac{n}{p}\right) + \left(1 - \frac{1}{p}\right) Q\left(\frac{n}{p^2}\right) \\ & + \ldots + \left(1 - \frac{1}{p}\right) Q\left(\frac{n}{p^{\varpi}}\right). \end{aligned} \right.$$

On aperçoit ainsi la formule générale suivante, dans laquelle φ désigne le symbole de l'indicateur (n° 216), et d un diviseur quelconque de D

$$(7)\quad G(n) = \sum \frac{\varphi(d)}{d} Q\left(\frac{n}{d}\right).$$

On peut démontrer la généralité de la formule (7) en faisant voir qu'elle est vraie pour la valeur D du plus grand codiviseur de $\alpha, \beta, \gamma, \ldots, \lambda$ lorsqu'elle est admise pour tout diviseur de D; on peut aussi démontrer directement l'exactitude de la formule (7), que l'on peut encore écrire sous la forme

$$(8)\quad G(n) = \frac{1}{n} \sum \varphi(d) R\left(\frac{n}{d}\right).$$

Le contenu de cette Note nous a été communiqué par M. le colonel C. Moreau.

VIII. — Sur les restes du triangle arithmétique (n° 228).

Nous avons déjà indiqué le moyen de calculer le reste de la division d'un terme quelconque C_m^n du triangle arithmétique de Pascal par un

nombre premier p, en ramenant les indices m et n à des entiers compris entre o et p. On peut encore simplifier cette recherche et ramener les indices à des nombres dont l'un ne dépasse pas $E\frac{p}{2}$, et l'autre $E\frac{p}{3}$, par les considérations suivantes, que nous avons tirées du Mémoire de CAUCHY. tout en simplifiant l'exposition et les démonstrations (*loc. cit.*, p. 231-243). Mais, pour la symétrie des calculs et pour leur extension à la détermination des restes des coefficients dans les puissances d'un polynôme, par un module premier p, il est préférable de remplacer le triangle de PASCAL par le carré arithmétique de FERMAT (n° 53).

Soit donc un terme quelconque

$$F_x^y = \frac{(x+y)!}{x!\,y!} = F_y^x,$$

nous pouvons supposer, par les formules du n° 228,

$$x+y<p-1 \quad \text{et} \quad x \leqq \frac{p-1}{2}.$$

D'autre part, si l'on désigne par x, y, z trois entiers positifs dont la somme égale $(p-1)$, on a

$$\frac{(x+y+z)!}{x!\,y!\,z!} = C_{p-1}^x\, F_y^z$$

ou, par la première formule de la page 420 et en raison de la symétrie,

$$\frac{(p-1)!}{x!\,y!\,z!} \equiv (-1)^x F_y^z \equiv (-1)^y F_z^x \equiv (-1)^z F_x^y \qquad (\text{mod.}\, p);$$

on en déduit

$$F_x^y \equiv (-1)^x F_x^{p-1-x-y} \qquad (\text{mod.}\, p).$$

Par la formule précédente, on peut supposer

$$y \leqq p-1-x-y \quad \text{ou} \quad y \leqq \frac{p-x-1}{2},$$

et, puisque $x \leqq y$, on peut supposer

$$x \leqq \frac{p-1}{3}.$$

Par conséquent, pour un module donné p, on construit le carré arithmétique de FERMAT par la loi de formation ordinaire, en ne conservant que les restes minimums pour des valeurs de x qui ne dépassent pas $E\frac{p}{3}$,

et pour des valeurs de y qui ne dépassent pas $E\frac{p}{2}$. On a, par exemple, pour $p = 19$.

F	1	2	3	4	5	6	7	8	y
1	2	3	4	5	6	7	8	9	
2	.	6	$\bar{9}$	$\bar{4}$	2	9	$\bar{2}$	7	
3	.	.	1	$\bar{3}$	$\bar{1}$	8	6	.	
4	.	.	.	6	$\bar{7}$	1	$\bar{7}$	.	
5	.	.	.	.	5	6	.	.	
6	.	.	.	.	.	$\bar{7}$	.	.	
x									

Restes du carré arithmétique de FERMAT par 19.

On vérifie les calculs en observant que, si l'on détermine, par la loi de formation, le terme qui suit le dernier de chaque ligne horizontale, on doit obtenir un reste égal et de signe contraire au précédent si x est impair, et égal à l'antéprécédent si x est pair.

Lorsque le module p dépasse 50, le Tableau des restes devient trop étendu; cependant, lorsque le nombre premier p ne dépasse pas 1000, on peut calculer les restes du triangle arithmétique par des additions, au moyen de Tables construites par JACOBI, et désignées sous le nom de *Canon arithmeticus*. La théorie et l'application de ces calculs seront exposées plus loin.

IX. — Sur le théorème de Staudt et Clausen (n° 234).

M. HERMITE a indiqué une méthode de calcul des nombres entiers A dont nous allons simplifier la démonstration, tout en lui laissant une forme plus générale. Cette méthode, dit l'illustre auteur dans sa Lettre à BORCHARDT (*Journal de Crelle*, t. LXXXI, p. 93), conduit à la connaissance d'un grand nombre de fonctions numériques venant se joindre à toutes celles dont la théorie des fonctions elliptiques a donné l'origine et les propriétés.

Soit un polynôme $f(x)$, à coefficients entiers, et

$$\varphi_r(x) = \frac{1}{r!}\left[\frac{d^r f(x+1)}{dx^r} - \frac{d^r f(x)}{dx^r}\right];$$

les polynômes $\varphi_r(x)$ ont aussi leurs coefficients entiers. Au moyen de la formule de TAYLOR, l'équation fondamentale pour le calcul des nombres de BERNOULLI (n° 135)

$$f(B+x+1) - f(B+x) \triangleq f'(x)$$

peut être écrite sous la forme

$$f'(x) = B_0\varphi_0 + B_1\varphi_1 + B_2\varphi_2 + \dots.$$

Si l'on remplace les nombres B en fonction des nombres entiers A fournis par le théorème de Staudt, on trouve, en posant

$$\Sigma_1 = A_0\varphi_0 + A_1\varphi_1 + A_2\varphi_2 + \dots - f'(x),$$

et pour p premier

$$\Sigma_p = \varphi_{p-1}(x) + \varphi_{2p-2}(x) + \varphi_{3p-3}(x) + \dots,$$

la formule

$$(1) \qquad \Sigma_1 = \Sigma_2 + \Sigma_3 + \Sigma_5 + \Sigma_7 + \Sigma_{11} + \dots.$$

D'ailleurs Σ_p est un nombre entier pour toute valeur entière de x, car, si la somme des fractions

$$\frac{a}{\alpha}, \quad \frac{b}{\beta}, \quad \frac{c}{\gamma}, \quad \dots, \quad \frac{l}{\lambda},$$

dont les dénominateurs désignent des nombres premiers différents, est égale à un nombre entier, chacune des fractions de la somme est égale à un nombre entier.

En supposant $f(x) = x^{2n-1}$, on retrouve les deux propositions de M. Hermite, savoir :

Les expressions

$$\frac{1}{p}\left(C_{2n+1}^{p-1} + C_{2n+1}^{2p-2} + C_{2n+1}^{3p-3} + \dots\right)$$

et

$$\frac{x^{2n+1}}{p}\left(\frac{C_{2n+1}^{p-1}}{x^{p-1}} + \frac{C_{2n+1}^{2p-2}}{x^{2p-2}} + \frac{C_{2n+1}^{3p-3}}{x^{3p-3}} + \dots\right)$$

sont des nombres entiers, si x est entier et p premier.

X. — Sur l'extraction des racines par les moyennes (n° 251).

Considérons deux nombres positifs quelconques a_0 et b_0; désignons par a_1 et b_1 la moyenne arithmétique et la moyenne harmonique des deux nombres donnés, de telle sorte que

$$a_1 = \frac{a_0 + b_0}{2}, \qquad b_1 = \frac{2a_0 b_0}{a_0 + b_0}, \qquad a_1 b_1 = a_0 b_0;$$

répétons les mêmes opérations sur a_1 et b_1, puis sur a_2 et b_2, et ainsi de suite, de telle sorte que l'on ait

$$a_{n+1} = \frac{a_n + b_n}{2}, \qquad b_{n+1} = \frac{2a_n b_n}{a_n + b_n}, \qquad a_{n+1} b_{n+1} = a_0 b_0;$$

les nombres $a_1, a_2, a_3, \ldots, a_n$ sont décroissants, mais leurs carrés surpassent le produit $a_0 b_0$; les nombres $b_1, b_2, b_3, \ldots, b_n$ sont croissants, et leurs carrés sont toujours plus petits que $a_0 b_0$. Enfin la différence $(a_n - b_n)$ décroît très rapidement jusqu'à zéro.

On obtient, de cette façon, un procédé rapide d'extraction de la racine carrée, qui était connu des anciens. La méthode d'interpolation par les parties proportionnelles, appliquée par HIPPARQUE à la détermination de l'équinoxe, y conduit directement. En effet, soit $a_0 > b_0$; en prenant la valeur b_0 approchée par défaut, on obtient pour le carré un nombre trop petit de $(a_0 b_0 - b_0^2)$; en prenant la valeur de a_0 approchée par excès, on obtient pour le carré un nombre trop grand de $(a_0^2 - a_0 b_0)$. Donc, en désignant par b_1 la nouvelle valeur de $(a_0^2 - a_0 b_0)$, dans la supposition des accroissements proportionnels, on aura

$$\frac{b_1 - b_0}{a_0 - b_0} = \frac{b_0}{a_0 + b_0},$$

d'où

$$b_1 = \frac{2a_0 b_0}{a_0 + b_0}.$$

Quant aux inégalités précédentes, elles sont immédiatement visibles sur une figure géométrique.

On peut exprimer a_n et b_n comme fonctions numériques du second ordre: en effet, si l'on pose (n° 177)

$$u^2 \triangleq pu - q,$$

avec

$$p = a_0 + b_0, \qquad q = \left(\frac{a_0 - b_0}{2}\right)^2,$$

on a les formules

$$a_n = \frac{V_{2^{n-1}}}{V_0 V_1 V_2 V_{2^2} \ldots V_{2^{n-2}}} = \frac{V_{2^{n-1}}}{2U_{2^{n-1}}} = \frac{a_0 b_0}{b_n},$$

$$\frac{1}{2}(a_n - b_n) = \frac{q^{2^{n-1}}}{V_1 V_2 V_{2^2} \ldots V_{2^{n-1}}}.$$

On peut appliquer un procédé analogue à l'extraction de la racine cu-

bique d'un produit $a_0 b_0 c_0$ de nombres positifs; on pose

$$\left\{\begin{aligned} a_1 &= \frac{a_0 + b_0 + c_0}{3},\\ b_1 &= \frac{b_0 c_0 + c_0 a_0 + a_0 b_0}{a_0 + b_0 + c_0},\\ c_1 &= \frac{3 a_0 b_0 c_0}{b_0 c_0 + c_0 a_0 + a_0 b_0} \end{aligned}\right. \quad \text{et} \quad \left\{\begin{aligned} a_{n+1} &= \frac{a_n + b_n + c_n}{3},\\ b_{n+1} &= \frac{b_n c_n + c_n a_n + a_n b_n}{a_n + b_n + c_n},\\ c_{n+1} &= \frac{3 a_n b_n c_n}{b_n c_n + c_n a_n + a_n b_n}. \end{aligned}\right.$$

On a d'ailleurs

$$a_{n+1} b_{n+1} c_{n+1} = a_n b_n c_n = \ldots = a_1 b_1 c_1 = a_0 b_0 c_0;$$

les nombres a_n, b_n, c_n convergent très rapidement vers la racine cubique du produit $a_0 b_0 c_0$.

Plus généralement, on a un procédé analogue pour l'extraction de la racine d'indice r du produit de r nombres positifs $a_0\, b_0\, c_0 \ldots l_0$.

Désignons par p_1 la moyenne arithmétique des n nombres $a_0, b_0, c_0, \ldots, l_0$; par p_2 la moyenne arithmétique des C_r^2 produits de ces nombres pris deux à deux, par p_3 la moyenne arithmétique des C_r^3 produits de ces nombres pris trois à trois, et ainsi de suite, de telle sorte que l'on ait l'identité symbolique

$$(x - a_0)(x - b_0)(x - c_0) \ldots (x - l_0) \triangleq (x - p)^r.$$

Posons ensuite

$$a_1 = p_1, \qquad b_1 = \frac{p_2}{p_1}, \qquad c_1 = \frac{p_3}{p_2}, \qquad \ldots, \qquad l_1 = \frac{p_r}{p_{r-1}},$$

il en résulte

$$a_1 b_1 c_1 \ldots l_1 = a_0 b_0 c_0 \ldots l_0.$$

Formons de nouveaux nombres a_2, b_2, c_2, $\ldots$, l_2, déduits de a_1, b_1, c_1, $\ldots$, l_1, comme ceux-ci ont été déduits de a_0, b_0, c_0, $\ldots$, l_0; nous obtenons ainsi des suites de r nombres $a_n, b_n, c_n, \ldots, l_n$, dont le produit reste constant, et qui convergent très rapidement vers la racine d'indice r du produit donné $a_0 b_0 c_0 \ldots l_0$.

L'application de ce procédé conduit à des formules fort importantes, que nous exposerons plus loin, dans l'application des fonctions elliptiques et abéliennes à la théorie des nombres.

XI. — Sur les réduites intermédiaires (n° 259).

Soit un nombre x développé en fraction continue; considérons deux réduites dont les indices diffèrent de deux unités

$$\frac{f_{p-1}}{g_{p-1}} \quad \text{et} \quad \frac{f_{p+1}}{g_{p+1}};$$

nous avons (n° **242**)

$$\begin{cases} f_{p+1} = q_{p+1} f_p + f_{p-1}, \\ g_{p+1} = q_{p+1} g_p + g_{p-1}; \end{cases}$$

posons, de plus,

$$\begin{cases} u_h = h f_p + f_{p-1}, \\ v_h = h g_p + g_{p-1}. \end{cases}$$

Si l'on donne à h les valeurs entières o, 1, 2, 3, ..., q_{p+1}, on obtient des fractions $(u_h : v_h)$, que l'on appelle *réduites intermédiaires;* on a la suite

$$\frac{f_{p-1}}{g_{p-1}}, \quad \frac{f_{p-1}+f_p}{g_{p-1}+g_p}, \quad \frac{f_{p-1}+2f_p}{g_{p-1}+2g_p}, \quad \ldots, \quad \frac{f_p}{g_p}.$$

On a ainsi formé, entre les réduites d'indices $(p-1)$ et p, une suite incomplète de Brocot, en intercalant d'abord une médiante entre les deux réduites, puis une autre médiante entre la médiante intercalée et la dernière réduite, et ainsi de suite. On a donc les propriétés suivantes :

1° Les réduites intermédiaires sont des fractions irréductibles.

2° La différence de deux réduites intermédiaires consécutives est égale à une fraction dont le numérateur est 1 et dont le dénominateur est égal au produit des dénominateurs des réduites.

3° Si l'on développe un nombre x en fraction continue, et si l'on intercale entre la suite des réduites de rang impair toutes les réduites intermédiaires, de telle sorte que les dénominateurs forment une suite croissante, on obtient une nouvelle suite croissante dont les fractions ne surpassent pas x. De même pour les réduites de rang pair.

4° On peut prolonger indéfiniment l'une des suites de réduites intermédiaires. En effet, si q_n désigne le dernier quotient incomplet, on peut introduire encore un quotient incomplet q_{n+1} plus grand que tout entier donné, et poser $q_{n+1} = \infty$. On forme ainsi une suite de fractions irréductibles qui s'approchent de x d'un nombre moindre qu'un nombre donné, si petit qu'il soit.

Les remarques précédentes permettent de déterminer, parmi toutes les fractions dont le dénominateur ne surpasse pas un nombre donné N, celles qui s'approchent le plus, par excès et par défaut, d'un nombre donné quelconque x. En effet, on développe x en fraction continue; si l'une des réduites a pour dénominateur N, c'est l'une des fractions cherchées; on forme alors entre cette réduite et la précédente une suite incomplète de Brocot, en ne conservant que les médiantes dont le dénominateur ne surpasse pas N. Si aucune des réduites n'a pour dénominateur N, on prend les deux réduites dont les dénominateurs comprennent le nombre N et l'on intercale entre elles une suite incomplète de Brocot.

Enfin, nous ajouterons que la considération des suites de Brocot et de Farey conduit immédiatement à la démonstration de ce théorème de Lejeune-Dirichlet :

Dans l'ensemble des fractions dont le dénominateur ne surpasse pas un entier donné N, *il en existe au moins une de dénominateur* q, *qui diffère d'une quantité moindre que* $\frac{1}{q\mathrm{N}}$, *par défaut ou par excès, d'un nombre positif quelconque* x.

ERRATA.

Pages	Lignes	*Au lieu de*	*Lire*
108	23	$3^4 \ldots\ 9911241$,	$3^{11} \ldots\ 40787$,
128	20	ax^2	x^2
183	formule (2)	$a^{p(p+1)}$	$a^{\frac{1}{2}p(p+1)}$
184	5	$(1+a^2x)\varphi(ax)$	$(1+ax)\varphi(a^2x)$
217	11	$\exp ax$	$\exp a$
220	5	$(2n-1)$	$(2n-2)$
220	6	$(2n-2)\mathrm{S}_{2n-2}$	$(2n-1)\mathrm{S}_{2n-1}$
235	formules (1) et (2)	diviser le second membre par 2	
253	formule (3)	$(2x+1)$	$(2x-1)$
259	5	$(1-y)^q$	$(x-y)^q$
283	23	$bcd \ldots l$	a_0
313	formule (1)	p^{n-r}	p^{n-2r}
377	avant-dernière	valeurs de a	valeurs de x
387	5	égale à une	égal à une
440	13	$a^4 = 1$	$a^4 = 1$,
440	avant-dernière	module q	module p

FIN DU TOME PREMIER.

TABLE DES MATIÈRES.

LIVRE I.

LES NOMBRES ENTIERS.

CHAPITRE I.

Addition des nombres entiers.

CHAPITRE II.

Soustraction des nombres entiers.

CHAPITRE III.

Multiplication des nombres entiers.

CHAPITRE IV.

Division et classification des entiers.

CHAPITRE V.

Les nombres figurés.

CHAPITRE VI.

L'analyse combinatoire.

CHAPITRE VII.

La Géométrie de situation.

CHAPITRE VIII.

La multiplication algébrique.

LIVRE II.

LES NOMBRES RATIONNELS.

—

CHAPITRE IX.

Les nombres fractionnaires.

CHAPITRE X.

Le calcul des probabilités.

CHAPITRE XI.

La division algébrique.

L'interpolation.

CHAPITRE XII.

Les polynômes dérivés.

CHAPITRE XIII.

Le calcul symbolique.

CHAPITRE XIV.

Sommation des puissances numériques.

CHAPITRE XX.

Les nombres premiers.

CHAPITRE XXI.

Les diviseurs des nombres.

CHAPITRE XXII.

De l'indicateur.

CHAPITRE XXIII.

Les restes.

CHAPITRE XXIV.

Les fractions continues.

Fractions continues généralisées.

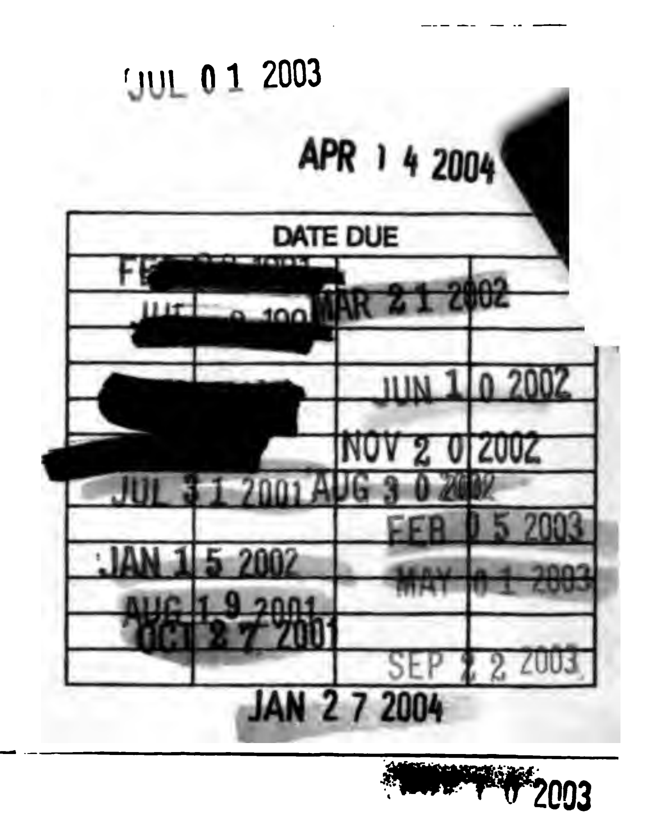
Intercalation et Médiation.

Sur l'équation $ax + by = c$.

NOTES ET ADDITIONS.

FIN DE LA TABLE DES MATIÈRES DU TOME PREMIER.

16897 Paris. — Imprimerie GAUTHIER-VILLARS ET FILS, quai des Grands-Augustins, 55.


JUL 01 2003
APR 14 2004
DATE DUE
[redacted]
MAR 21 2002
JUN 10 2002
NOV 20 2002
JUL 31 2001
AUG 30 2002
FEB 05 2003
JAN 15 2002
MAY 01 2003
AUG 19 2001
OCT 27 2001
SEP 22 2003
JAN 27 2004